INVESTIGATING HASTILY-FORMED COLLABORATIVE NETWORKS

THESIS

Joshua S. Campbell
Captain, USAF

Stanley L. Cooley
Lieutenant Commander, US Navy

Matthew F. Durkin
Major, USAF

Brian K. Maddocks
Major, USAF

AFIT/GSE/ENY/07-M01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GSE/ENY/07-M01

INVESTIGATING HASTILY-FORMED COLLABORATIVE NETWORKS

THESIS

Presented to the Faculty
Department of Aeronautics and Astronautics
Graduate School of Engineering and Management
Air Force Institute of Technology
Air University
Air Education and Training Command
in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Systems Engineering

Joshua S. Campbell, BS
Captain, USAF

Stanley L. Cooley, BS
Lieutenant Commander, US Navy

Matthew F. Durkin, BS
Major, USAF

Brian K. Maddocks, BS
Major, USAF

March 2007

AFIT/GSE/ENY/07-M01

INVESTIGATING HASTILY-FORMED COLLABORATIVE NETWORKS

Joshua S. Campbell, BS
Captain, USAF

Stanley L. Cooley, BS
Lieutenant Commander, US Navy

Matthew F. Durkin, BS
Major, USAF

Brian K. Maddocks, BS
Major, USAF

Approved:

Lt Col John M. Colombi (Chairman) Date

Maj Jörg D. Walter (Member) Date

Maj Laura R. C. Suzuki (Member) Date

AFIT/GSE/ENY/07-M01

Abstract

This research explores both the human and technical aspects of the network centric environment in the context of a major disaster (e.g. Hurricane Katrina) or incident of national significance. The National Incident Management System (NIMS) is viewed by the authors as a social network, and an organizational topology is developed to improve its effectiveness. A Rapid Network Deployment Kit (RNDK) using commercial-off-the-shelf (COTS) wireless networking technology is also proposed that facilitates immediate NIMS implementation. The integration of logical and technical analyses forms a comprehensive systems engineering proposal to facilitate collaboration in a net-centric environment. It is envisioned that the methodology used herein to derive and evaluate comprehensive networks proves extendable to other contexts thereby contributing to the net-centric body of knowledge.

Table of Contents

Page

List of Figures

Figure Page

Figure Page

List of Tables

INVESTIGATING HASTILY-FORMED

COLLABORATIVE NETWORKS

I. Introduction

1.1 Background

Recent disasters have highlighted the deficiencies in how Emergency Response Personnel (ERP) access and distribute vital information to one another. This problem is particularly apparent when incidents involve multiple agencies and multiple jurisdictions. Incompatible communications equipment as well as poor and/or differing incident management techniques have been identified as the primary culprit. Although the National Incident Management System (NIMS) has been mandated for use by all Emergency Response Agencies (ERA) as a means to better facilitate incident management, the Department of Homeland Security has shown little improvement in fixing the interoperability issue. The NIMS solution to incident management involves a comprehensive national plan, which involves the potential coordination of agencies from the Local, State, and Federal levels. The primary enabler of this solution is the requirement for all potential participating response agencies to communicate with one another and have access to pertinent information as needed. DHSs Office of Interoperability and Compatibility (OIC) states that in order to fulfill this requirement, access to voice, as well as data communication capabilities are required. Unfortunately, the means to accomplish this level of sophistication are not currently realized. Many of the more than 60,000 ERAs throughout the Nation still rely on voice- only analog equipment to provide their emergency communication networks. Furthermore, these systems normally only operate in one of the three frequency bands currently in use by various agencies throughout the country for emergency response communications. New standards from DHS attempt to alleviate the interoperability problem by pushing for new digital radios able to implement specific protocols, operate in multiple bands, and thus ensure interoperability. However, the cost of approximately $2000 per handheld radio, plus the cost of the supporting infrastructure, prevents many agencies from purchasing the equipment.

The first hours following a major incident can be the most crucial for ERP to prevent loss of life, curtail rioting and looting, and prevent further exacerbation of the incidents impact. Coordination among response agencies is a must, and requires reliable communications. However, following large-scale natural disasters, existing and supporting infrastructure normally relied upon for response coordination and information sharing have been destroyed. The result is that ERP are left with very little, if any means of communicating with one another and their supporting agencies. This situation was seen in New Orleans following Katrina as ERPs from multiple agencies and jurisdictions entered the city without the direction and coordination normally provided by the Incident Command System (ICS). This led to a major breakdown in the overall disaster management of the situation, and thus prevented help from getting to the needed locations. The following was taken from an Associated Press article.

> …first responders were simply unable to share essential information. Federal emergency management officials claim they didn't know for days about thousands of people camped out, thirsty and hungry, at the New Orleans convention center. Rescuers in helicopters couldn't talk to crews patrolling in boats. National guard commanders in Mississippi had to use runners to relay orders [32].

Even agencies with compatible equipment were limited in communications as the loss of repeater towers prevented long range transmissions and the loss of the supporting trunk systems allowed for only a handful of mutual aid channels to be used. One report stated that only about two or three of these channels were available while more than 4,000 personnel were attempting to use them. These channels quickly became overwhelmed, thus preventing any type of effective communication [32].

As a result of the many issues seen in recent disasters, many organizations and companies are developing new solutions, which can be used to provide communications in the event of a destroyed or unavailable support infrastructure. However, there are two major problems with many of the proposed solutions. First, some approaches revolve around attempting to provide repeaters and trunking for the plethora of radio equipment being used by responders. While this solution provides emergency response communications, it does nothing to enhance compatibility. Other approaches use sophisticated patching or gateways to allow the various array of devices to communicate. However, the complexity of these systems leads to excessive delays in their deployment following a major incident. Arguably, the most crucial time following a disaster is the first few hours. It is during this time that first responders disperse through the community to provide emergency service to those in urgent need. The lack of critical communications could mean the difference between life and death.

Assuming vital communications have been restored to an area, there still exists an issue of managing the incident response efforts. The coordination of multiple agencies can be very complex and the tactics used by incident commanders may be significantly limited by the communication capabilities he has. Therefore, strategies must exists prior to an emergency which afford responders the opportunity to independently organize and collaborate without the need of direction. In this way, tactics can best utilize technologies available to both the incident commander and different responders.

1.2 Problem Statement

A comprehensive review of the Katrina response literature reveals the following recurring problem areas:

1. Responders were unable to communicate.
   (a) Physical communications infrastructure was destroyed resulting in line of site only communications.

   (b) Temporary Communications Systems required excessive time and infrastructure to become operational

   (c) Communications systems as a whole were not interoperable.

2. Responders were hesitant or unable to communicate outside normal channels.

   (a) Situational awareness suffered due to low information sharing.

   (b) Information was lost.

3. Collaboration and coordination of efforts did not effectively occur

   (a) Vast pools of resources remained idle as coordination with them did not or could not take place.

   (b) Volunteers haphazardly found tasks to help with, sometimes contributing to the chaos.

Effective communications require interoperable systems, the transfer of information (i.e. data, ideas, and emotions), and the subsequent appropriate processing of the transferred information by the receiver. A compatible network can guarantee a channel in which information can flow, but it cannot guarantee the appropriate processing of the information. Therefore, without the processing, communications have not been fully achieved but rather we have only passed data from one place to another.

If we assume the goal of global interoperability is achieved, then what? Techniques must be found to manage the vast amount of information flowing over this common network to ensure hindrances to effective communications, such as information overload, bandwidth limitations, and network delays are minimized. Traditional emergency response systems utilize voice radio transmissions over a number of channels to manage network traffic. However, as the number of users on each channel grows, so does the amount of non-significant traffic and network delays observed by each user. Thus, as the number of communication channels increase the amount of the globally shared information will likely decrease. The result of this is a net lowering of shared situational awareness. Voice based communications networks suffer the catch 22: more channels equate to smaller traffic delays and less chance of information overload by each user but result in a reduction of global information sharing. Fewer channels increase global information sharing, but may increase network delays and the chance of information overload. Another method commonly used to try to improve voice network communications (whether directly or indirectly) is the use of a hierarchical Command and Control (C2) structure. Hierarchical structures translate to specific persons having relatively high data sharing capabilities with lower nodes and specific nodes above. This results because information is aggregated as it flows up the chain of command but is filtered as it flows down. In order to achieve the most efficient and effective disaster response, new systems and techniques must be implemented to optimize communications. This thesis examines how the naturally formed networks of responders sent to deal with various incidents can be enhanced to better optimize global situational awareness, incident responses, and allowing the responders to have enough bandwidth to communicate with each other as necessary while still minimizing the overall strain on the command and control structure. In order to accomplish this, this research seeks to draw a parallel between the domains of major disasters and modern warfare, demonstrating how network-centric operations (NCO) theory can be applied to disaster response to create shared situational awareness, self-synchronization, and ultimately improved mission effectiveness.

1.3 Research Objectives

The objective of this research is to facilitate efficient and effective interoperable communications in the wake of a major disaster. The research objectives focus on proposing a system made up of todays technology that can be rapidly deployed as well as proposing an organizational structure that can work well under the conditions present following a major disaster.

1.3.1 Objective 1, Physical Network Design. The first objective of this research is to propose the design for a Rapid Network Deployment System (RNDS), which facilitates a hastily formed, interoperable, responder network in the wake of a major incident. The RNDS architecture will develop through the consideration and examination of wireless technologies, including 802.11 (also known as Wireless Fidelity or Wi-Fi), and 802.16 (also known as Worldwide Interoperability for Microwave Access or WiMax). Furthermore, the system architecture will not make any assumptions concerning existing communications infrastructure in an incident location, and will therefore, attempt to provide a total and independent solution for personnel working in the area. Kevin Ross, Assistant Director for Technology, New York State Emergency Management Office states:

> From Katrina, we learned that we cannot rely on any specific infrastructure: PSTN, radio tower, or other. We need the option of reconstituting communications from a disaster recovery site that is on a different power grid, with different phone providers [13].

The proposed system will comply with the requirements set forth in the NIMS regarding support of the incident command and control structure and the SAFECOM Statement of Requirements (SoR) regarding public safety communications. Furthermore, the solution will support the knowledge management tenants of net-centric operations.

Questions to be answered in this thesis include:

- What features are needed in the design of the RNDS to facilitate a hastily formed network in the wake of a disaster?
- Can a wireless communications system for emergency disaster response, be implemented using 802.11, and 802.16 technologies?
- How well does the system meet the requirements for a public safety communications network, as set forth in the NIMS and SoR?
- Can a kit be developed which contains the key nodes for network implementation while remaining transportable by a small vehicle?

1.3.1.1 Hypotheses for objective 1. It is the authors' belief that recent advances in wireless technologies can be used to develop a temporary rapidly deployable and interoperable communications network, which meets the requirements set forth in the NIMS, and SAFECOMs SoR. A wide array of systems and technologies are available today with varying features. However, it is believed that 802.11 and 802.16 technologies provide a cost effective, interoperable solution to the hastily formed network problem. A further goal of this technical solution is to utilize concepts associated with systems engineering to evaluate the proposed design of the hypothesized system.

This research accesses the current capability of the existing IEEE 802.11 and 802.16 standards to provide a rapidly deployable network for responders. The primary goal of the assessment is to acquire the capability of the systems in order to describe the design needed for the RDNS. Therefore, the focus is not on determining detailed technical specifications, but rather on the general capability of the technologies and what role they play in the overall solution architecture.

An investigation of the capabilities of the current 802.11 and 802.16 technologies will be conducted. Next, Department of Defense (DoD) and Department of Homeland Security (DHS) documents are researched to help determine the capabilities and tasks needed for a communication system to enable netcentricity. The proposed systems capabilities will then be compared with those identified in the research. A review will then be conducted to determine the effectiveness of the proposed solution for a rapidly deployable and interoperable communications system.

1.3.2 Objective 2, Logical Network Design. The second objective of this research is to:

1. Develop the empirical foundation for an organizational structure using NCO concepts and graph theory metrics.
2. Computationally model the structure using the disaster response context.
3. Analyze the model metrics and explain results.

4. Explain how the physical implementation of communication equipment can add to or detract from global situational awareness.

1.3.2.1 Approach. The first step is building a model that will describe disaster response as a graph where responders and command and control are vertices with attributes that correspond to the various tasks in the affected area. The model consists of three layers. The top layer is the organizational/people layer. The vertices in this layer represent responders assigned to tasks in the affected area and the command and control entities to whom the responders report. These same command and control entities also serve as the problem resolution point for issues that cannot be solved by a responder entity independently. The vertices in this layer are linked by edges that represent communications paths between entities in the organization. At this organizational/people layer communications edges are based on the organizational structure. Initially the edges are bidirectional from one level of hierarchy to the next. This serves as the baseline graph for this layer. The next layer is the physical layer. The vertices in this layer are again responders and the associated command and control entities. The links between any two vertices represent the ability of vertices to communicate based on the physical communications equipment available. The baseline for this layer of the network is a fully connected graph. Excursions that eliminate edges are conducted to determine the effects of incompatible equipment and damaged physical infrastructure. The third layer is the process layer. This layer represents the rules governing which responders should be able to collaborate without going through command and control (C2).

1.3.2.2 Use Cases. The following scenarios are considered in the model:

- Scenario 1: Baseline case.
    - Organizational layer: Responders are only allowed to connect to their assigned C2.
    - Physical layer: This layer has fully connected, ubiquitous communications.

    - Process layer: All information a responder receives or sends is to or from C2.

- Scenario 2:

    - Organizational layer: Responders are only allowed to connect to their assigned C2.
    - Physical layer: This layer has fully connected, ubiquitous communications.
    - Process layer: Responders are grouped by proximity. 50% of the information sent from responder is to command and control and 50% goes to other responders in the same proximity group.

1.4 Scope, Assumptions, and Limitations

This research is focused on evaluating the possible ways of organizing the communication patterns of a network of responders. Disaster relief operations, Hurricane Katrina Relief in particular, provide a context for studying this problem, however, the results of this research are not intended to be a recommendation for changing the National Incident Management System, Incident Command System or the way functional experts perform their specific tasks. Furthermore, this research is not intended to propose a specific material solution to the problem of disaster relief communications.

II. Literature Review

2.1 Overview

The problem of creating hastily-formed collaborative networks is investigated in the context of disaster response in this thesis. This problem has both a technical and a knowledge management aspect. The National Incident Management System (NIMS) is briefly described along with a survey of problems discovered with it in the wake of 9/11 and Hurricane Katrina. A common finding in these reports is that there is an overall lack of communications system interoperability nationwide throughout the disaster response community. These reports as well as current issues and initiatives in public safety communications are discussed below. A hypothesis of this thesis is that there is an organizational aspect of this problem as well. The basis of this hypothesis is the authors' familiarity with the area of network-centric operations (NCO). The analogy drawn between the domains of warfare and disaster response are substantiated, and relevent research in NCO theory is presented.

2.1.1 The National Incident Management System. The system under consideration in this research is based on the NIMS, which is "a consistent, nationwide approach to domestic incident management that is applicable at all jurisdictional levels and across funcitonal disciplines in an all-hazards context [25:p. 1]." Specifically,

> [The] system will provide a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State, and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system; multiagency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources [25:p. 1-2].

Research suggests that the major problem in implementing the NIMS during a major disaster or incident of national significance is inability to communicate. A typical example of this body of work is a study that considers, among other jurisdictions, Arlington County's After Action Report for the 9/11 disaster. This study identified "voice-oriented communications, limited situational awareness, and interoperability [as] three major problem areas of emergency response prevalent across the country [8:p. 255]." Analysis of the Hurricane Katrina response shows that the same problems existed almost four years after 9/11 and still exist today.

2.1.2 Hurricane Katrina Response. Hurricane Katrina is one of largest natural disasters in U.S. history. The storm's destruction covered approximately 90,000 square miles of Louisiana, Mississippi, and Alabama. This incident stressed the capabilities of National Response Plan (NRP) and Incident Command System revealing numerous weaknesses in the nation's ability to deal with a catastrophic event [39:p. 4].

Government Accountability Office (GAO) analysis of the challenges evident in the Hurricane Katrina response reveals four areas for improvement:

- Clearly defining and communicating leadership roles, responsibilities, and lines of authority for response in advance of a catastrophic disaster
- Clarifying the procedures for activating the National Response Plan and applying them to emerging catastrophic disasters
- Conducting strong advance planning and robust training and exercise programs
- Strengthening response and recovery capabilities for a catastrophic disaster [65].

The last of these areas, strengthening response and recovery capabilities, includes emergency communications [65:p. 9]. Katrina caused widespread damage to existing communications infrastructure including landlines and cellular telephone towers resulting in oversubscription on emergency radio systems. Loss of robust communications capabilities prevented communication between local, state and federal responders slowing the upward flow of situational awareness information discovered at the local level. This further inhibited responder ability to establish broad situational awareness regarding the extent of the damage due to lack of feedback.

The GAO report indicates that the first priority of disaster response agencies should be to establish operable telecommunications with sufficient capacity to meet everyday and emergency communication requirements. The second priority should be ensuring interoperability between and service agencies in real time. Hurricane Katrina rendered much of the existing telecommunicaitons infrastructure in Louisiana, Mississippi, and Alabama useless making real-time communication within and between agencies impossible. The GAO report cites this as one area where military capabilities could be used [65:p. 17].

Although the military response to Katrina was massive, the forces that arrived in theater did not integrate well with local and state responders. State plans for integrating federal resources did not anticipate the numbers of federal responders that flooded the area, and had no way of tasking or tracking them. Furthermore, most military communications equipment was not compatible with civilian systems. In some cases mobile communications vans that could connect incompatible systems were available but not adequately coordinated. Some sites had multiple systems while others had none. Adding to this challenge were restrictions placed on some of the deployed National Guard assets that their equipment could only support the sending state's units. The lack of communication did not in many cases prevent military units from acting on their own, though it did prevent communication up the chain regarding the status of ongoing missions and what new missions needed to be resourced [33:p. 25-26].

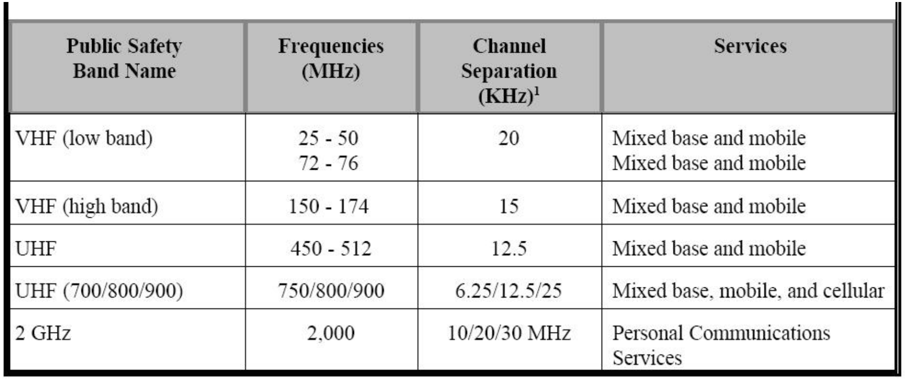
This requirement for improved communication capabilities is not new. Prior to Katrina the Department of Homeland Security listed interoperable communications along with strengthened information sharing and collaboration as two of the seven priorities for enhancing national first responder preparedness [39:p. 10]. In testimony before the Little Hoover Commission about the challenges of responding to major emergencies, the GAO expounded upon the need for interoperability, stating that effective communications is not necessarily the ability to talk with everyone all the time, but “the ability to talk with whom you want, when you want, when you are authorized [39:p. 6].”

This chapter first addresses the issue of fully interoperable communications that would allow anyone in the network to communicate with anyone else. Such an infrastructure, or infostructure, is the first step in solving these problems. As the GAO report points out, though, ubiquitous communications are not the end-all solution. Decisions about who communicates with whom, when, and about what are also needed to provide *effective communications*.

2.2 Public Safety Communications

2.2.1 Overview. There are more than 18,000 law enforcement agencies and 32,000 EMS agencies in the United States [28]. The vast majority of them utilize communication systems that underwent a stove-piped acquisition process. The result is fragmented Public Safety community with very little interoperability between systems. These systems operate in various frequency bands as well as use various, incompatible technologies. In order to better understand the current environment of Public Safety communications, a discussion of some of the differing methods and technologies for communicating follows. Some of the technologies are somewhat simple but lessons can be learned from them concerning the design of future systems. Table 2.1 shows a list of the common frequencies used by public safety agencies:

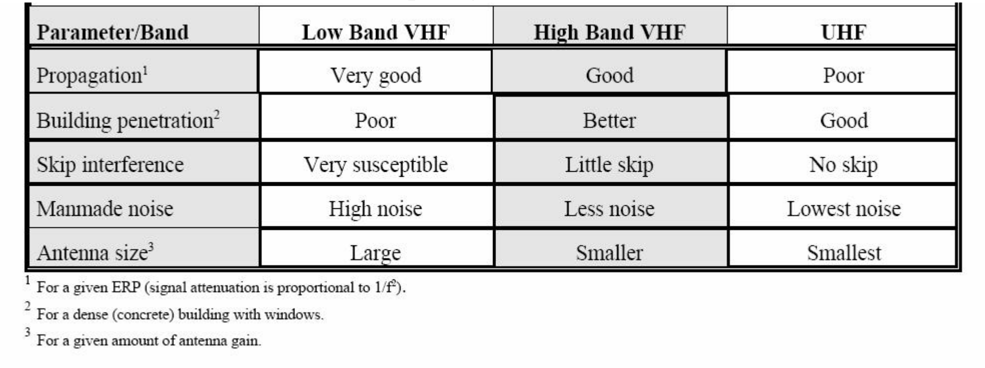
Table 2.1: Public Safety Frequencies [37]



Public Safety Band Name	Frequencies (MHz)	Channel Separation (KHz)[1]	Services
VHF (low band)	25 - 50 72 - 76	20	Mixed base and mobile Mixed base and mobile
VHF (high band)	150 - 174	15	Mixed base and mobile
UHF	450 - 512	12.5	Mixed base and mobile
UHF (700/800/900)	750/800/900	6.25/12.5/25	Mixed base, mobile, and cellular
2 GHz	2,000	10/20/30 MHz	Personal Communications Services

Each of the various frequencies has its advantages and disadvantages. In particular, low frequencies have longer wavelengths and tend to propagate further. However, they are more susceptible to atmospheric disturbances. On the other hand, high frequencies are less susceptible to atmospheric disturbances, but have a relatively short communications range. Other criteria for frequency selection are summerized in Table 2.2.

Table 2.2: Frequency Selection Criteria [37]



Parameter/Band	Low Band VHF	High Band VHF	UHF
Propagation[1]	Very good	Good	Poor
Building penetration[2]	Poor	Better	Good
Skip interference	Very susceptible	Little skip	No skip
Manmade noise	High noise	Less noise	Lowest noise
Antenna size[3]	Large	Smaller	Smallest

[1] For a given ERP (signal attenuation is proportional to $1/f^2$).

[2] For a dense (concrete) building with windows.

[3] For a given amount of antenna gain.

The UHF and VHF bands have traditionally had the most usage by public safety agencies. However, newer systems tend to operate in the 800 Mhz range as well as the 2.4 Ghz range. These higher frequencies allow for more channels to be used within the band. However, the two frequency bands are also shared with other common devices such as cell phones, cordless phones, and WiFi devices. As seen in 2.2, the channel separation in the 800 Mhz band ranges from 25 Khz down to 6.25 Khz. Small channel separation leads to lower amounts of available bandwidth within the channel. Bandwidth can be seen as the amount of information carrying capacity of a channel. The higher the bandwidth, the more information can be sent over the channel. Originally, the Federal Communication Commission (FCC) authorized the 25 Khz channel separation. But, due to overcrowding of the spectrum, the FCC is now requiring future systems to operate with 6.25 Khz channel spacing. This move will allow for more available channels, but at a cost of bandwidth. Future communications systems will have to be designed to handle large amounts of traffic, including voice, video, images, and text. Therefore, the use of higher frequencies which support greater channel and bandwidth proportions need to be considered in the design of new communications systems.

2.2.2 Transmission Methods. The two primary methods for data transmission are analog and digital. Emergency response radio systems throughout the Nation use both of these techniques to communicate. However, the two transmission methods are not directly compatible. The use of special equipment is needed to convert between the two. Analog transmissions involve the use of a continuous wave to communicate across the medium. Human voice is an example of a signal, which is traditionally transmitted with analog technology. Typical speech ranges in frequency from about 300 to 3000 hertz. With analog transmission, a resulting speech waveform is modulated via various techniques, onto a frequency called the carrier, and then transmitted. At the receiving end, the signal is de-modulated, or separated from its carrier, and consequently heard through a speaker device. The device responsible for the modulation and demodulation is called a modem.

With digital transmission, signals are transmitted across the medium in a series of discrete waveforms. All data is represented as a series of 1s or 0s, which could be interpreted as a set of positive and negative voltages. This series of positive and non-positive waves are transmitted and reproduced to its original state at the receiver. Voice can also be transmitted digitally by using a process called sampling and amplitude quantization to reproduce the analog waveforms shape. The analog waveform of a voice signal is sampled, or measured at very small, constant intervals, typically 8,000 times per second. As the number of samples per interval increase, so does the accuracy of the analog waves reproduction. Next, the measure samples are quantized, which means that they are converted to a form to be stored digitally. These digital signals are then transmitted to the receiver.

Digital transmission has distinct advantages over analog transmission methods. In particular, as an analog signal propagates through the medium, its quality begins to gradually decrease with distance as the signal power decreases and the signal noise increases. Thus the signal becomes more difficult to understand. However, the discrete nature of digital signals allow for them to be interpreted clearly up to the point where signal power fall below the detectable threshold. This threshold is normally at a further range than where analog signal can be detected (Figure 2.1).

Figure 2.1 shows a list of the common frequencies used by public safety agencies:

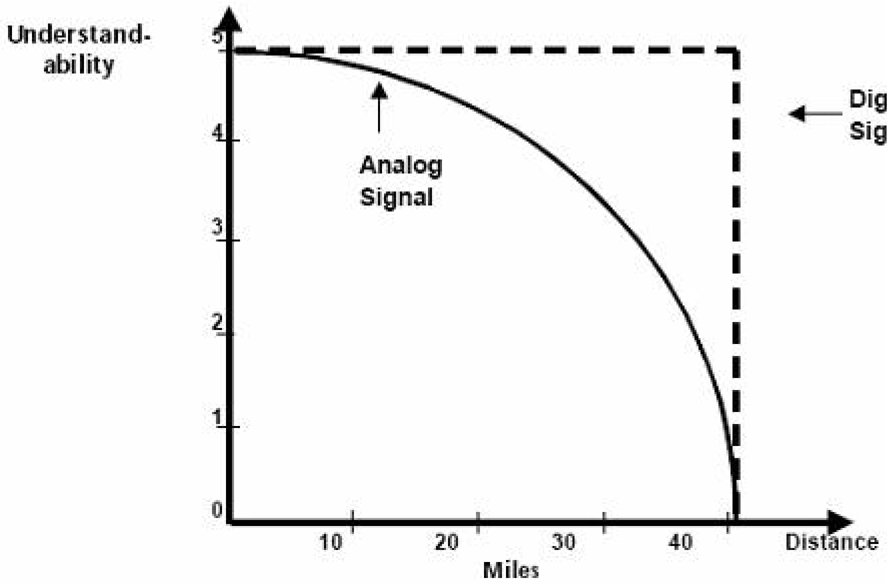


Figure 2.1: Analog versus Digital Propagation Distance [37]

The capability to transmit binary is part of the new P25 standard being dictated by the Department of Homeland Security for public safety radios. This new capability will allow emergency response agencies to better gain wireless access to the web, as well as allow for efficient transmission of data across the wireless medium.

2.2.3 Communications Systems. There are a number of systems in use today by Public Safety agencies for communications. These systems can be linked together to cover very large distances. For example, an entire portion of a state may be using one of the many systems to provide communications to its emergency response personnel.

The following examples represent the underlying concept of how each individual system works.

2.2.3.1 Simplex systems, non-repeater . Simplex radio systems operate on a single frequency at a time. They are essentially “walkie-talkie” type devices in which a user transmits over the frequency. Every other user on the same frequency will hear the transmission, as long as they are within reception range of the signal. The typical effective range of simplex radio systems is 2-4 miles line of sight. In order to increase range coverage, a central base station, which normally monitors all frequencies in use, has its antenna elevated. If two users, who are out of range of one another, wish to communicate, they must relay their transmissions through the person operating the base station. Therefore, mobile to base station communications are the most efficient ways to ensure all users on a channel hear the communications. Figure 2.2 shows a typical simplex radio communication system.

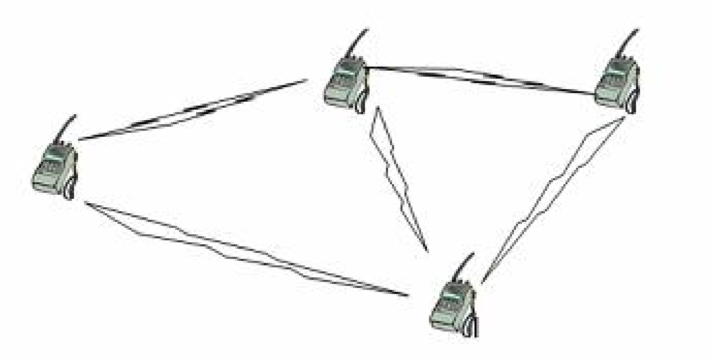


Figure 2.2: Simplex Radio Communications

2.2.3.2 Simplex system, repeater. Simplex radio systems can utilize a repeater device to extend communications ranges. The repeater is placed at an elevated point in the operating area and transmits at high power settings to ensure longer-range coverage. The system requires two different frequencies to operate. If a user wants to talk to another user, he transmits on one of the frequencies. The repeater hears the transmission, amplifies it, and rebroadcast it on a second channel. All radio in the

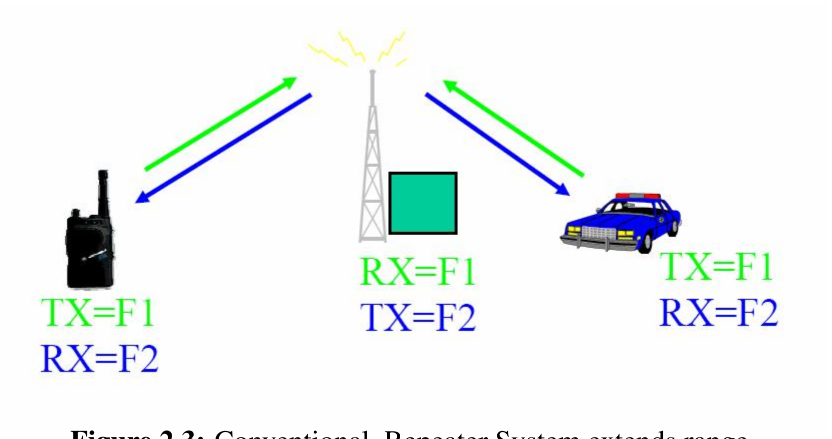


Figure 2.3: Conventional, Repeater System extends range.

reception area of the repeater will receive the transmission. Figure 2.3 depicts how a conventional repeater system works. In general, the repeater extends the effective range of radios, thus allowing more users to share the channel.

Repeater based simplex systems suffer from the same problem as non-repeater based systems. Since many users are sharing the same channel, a person has to wait his turn before he can speak. This problem increases rapidly as the number of users grows, when the average length of a transmission increases, or the frequency of transmission increases.

2.2.3.3 Trunk System. Trunk radio systems where designed to provide more efficient usage of the available channels assigned to an agency. Personnel using a trunk radio system are divided into user-groups. Instead of each user group being assigned to a specific channel for coordination purposes, the system automatically and dynamically assigns channels to users, based on demand. Take for example a small town, which has five fires in progress at the same time and in close proximity. Each fire incident requires a single channel for coordination purposes. If the responding agency were assigned only four channels for usage with a simplex system, two of the incidents would have to share channels. However, with a trunk radio system, each of the personnel at a particular incident would be assigned into a user group. Even though there are five user groups and three frequencies, there is not a problem. In a trunked system, the channels are not assigned, but rather exist as a pool of resources to be used as needed. So, if a person in a particular user group wishes to communicate, the system automatically finds an unused channel and provides it for use to the group. When the user stops talking on the channel, it goes back into the pool of resources. In order to get access to a channel, when the user presses his button to talk, a short message is sent on a control channel to the trunking system. The message contains the users group identification and indicates a desire to talk. The system then automatically assigns the frequency. The entire process happens very quickly and a user can generally start communication within one quarter of a second, providing a channel is available. In general, trunking system allow for more users to communicate effectively on a fewer channels. The major companies providing trunked systems to agencies include Motorola (SmartNet and Astro P25 Trunking), MA-Com (Enhanced Digital Access Communications System (EDACS) and a system known as OpenSky), and E.F. Johnson Trunking (MultiNet) [56]. These systems are primarily proprietary solutions, which may not be interoperable with one another. Figure 2.4 shows a trunked radio system.

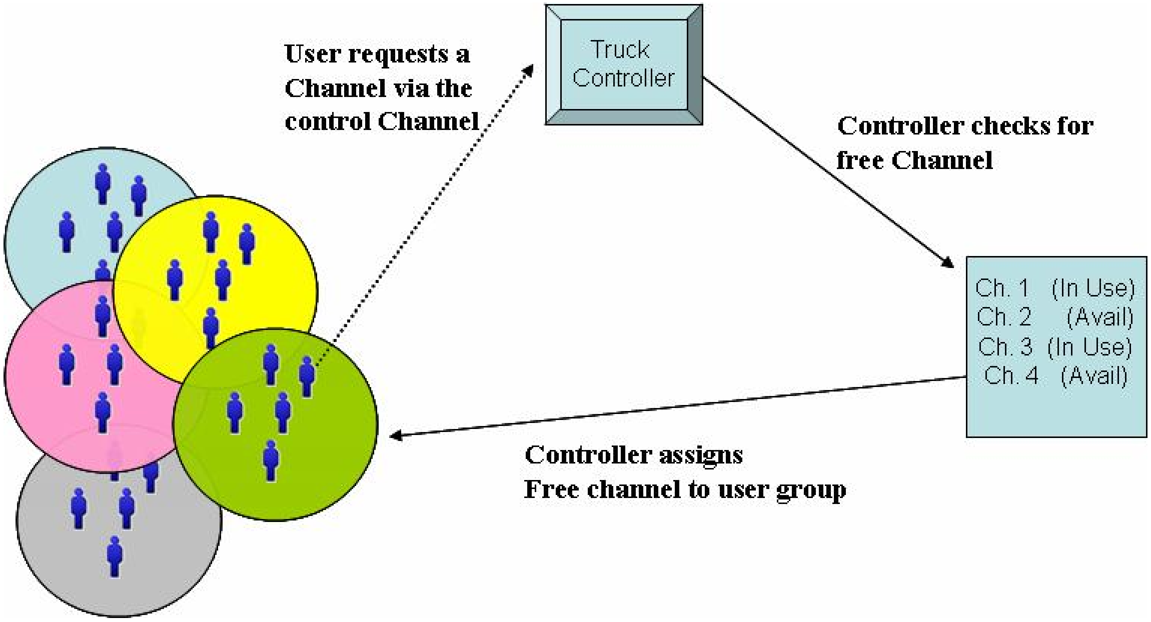


Figure 2.4: Trunked System Operation

2.2.4 Efforts for Interoperability. There are a number of systems and strategies in use today by agencies to try to obtain interoperability. Simple solutions consist of agencies exchanging some of their radios with each other on an as needed basis, or permanently loaning radios to neighboring agencies. Other solutions consist of utilizing stationary or vehicle-mounted equipment, which incorporates patching hardware and software, to interconnect varying systems. Agencies with the capital to do so may also purchase radios that have limited patching capabilities built in them. However, patching techniques can have certain drawbacks, including annoying transmission delays as the system performs its interconnections. This often results in the truncation of the beginning of transmissions. Also, the patching system often does not relinquish the channel immediately following a transmission over a trunked system. The result is channel access delays as experienced by users. There are also certain features of trunked systems that do not perform well over patches. All in all, patching techniques have had mixed success in public safety communications [56]. The better solution is to build with interoperability from the ground instead of trying to link incompatible devices together. This research utilizes DoD capabilities analysis methods to suggest a solution to the interoperability problem.

2.3 Organizational Aspects and Network Centric Operations

While interoperable communications equipment is one of if not the most significant problem surrounding NIMS implementation, it is not the only one. A working hypothesis of this research is that there is an organizational component as well. Compagnoni suggests that the complexity of a major disaster response is analogous to that of modern warfare, and points toward the U.S. military's network-centric operations (NCO) theory as an avenue of approach to the problem. The NCO body of knowlege supports this research by describing a dual-pronged approach consisting of both human and technical aspects [20]. This approach is also consistent with systems engineering best practices, which specify defining both functional (human) and physical (technical) architectures that combine to form a complete operational architecture.

2.3.1 Network-Centric Operations Theory.

Application of the Department of Defense's (DoD) NCO theory to the NIMS is suggested by Compagnoni who both participated in and subsequently studied the Hurricane Katrina response. He finds the top-down hierarchy described in the NIMS to be unresponsive in the chaos of a major disaster, and suggests application of net-centric and knowledge management concepts at the local level. He described the NIMS as

> an inverted pyramid of resources–ultimately, all resources come to rest on the local jurisdiction and under the leadership of the Incident Commander who must instantly integrate the vast network of resources [16:p. 3].

Local Incident Commanders are neither organized, trained, nor equipped to digest the glut of resources sent to local jurisdictions as seen in the Hurricane Katrina response. He concludes that "this approach fails to display the agility and flexibility needed at the *tactical* level of a major disaster [16:p. 60]."

A solution proposed by the DoD to create agile organizations is NCO theory. NCO begins with the Tenets of Net-Centric Warfare, which state:

- A robustly networked force improves information sharing.
- Information sharing and collaboration enhance the quality of information and shared situational awareness.
- Shared situational awareness enables self-synchronization.
- These, in turn, dramatically increase mission effectiveness [2:p. 5].

As evidenced in the first bullet, NCO theory views organizations as networks of people and suborganizations. These people/suborganizations, represented as nodes in the network, relate to and communicate among one another in some formal way. These relationships are represented as links, or edges, between the nodes. Together, nodes and edges form the network's topology, which affects the organization's performance. According to Alberts,

> networks with different characteristics correspond to different organizational structures that inherit the characteristics of the network...How organizations function is affected by the connections that exist or do not exist, and how these connections are utilized [1:p. 182].

When one thinks of a hierarchical organizational structure or topology, one usually thinks of an "org chart" with the boss at the top, the workers at the bottom, and lines of authority and communication running vertically. This structure is typical of both governmental (e.g. NIMS) and private sector organizations that evolved over the past 200 years, beginning with the industrial revolution. Its topology is hierarchical, and it is often referred to as "Industrial-Age." The concept was conceived by Adam Smith and perfected by Henry Ford and Alfred Sloan to manage the complexity of mass production. This structure evolved in and was reinforced by a predictable mass market of the latter 20th Century. In their groundbreaking work on business process reengineering, Hammer and Champy illucidate the following:

> The reality that organizations have to confront [now], however, is that the old ways of doing business simply don't work anymore. Suddenly the world is a different place...nothing is constant or predictable [35:p. 18-20].

In their work on NCO theory, *Power to the Edge*, Alberts and Hayes similarly conclude that

> if the situation/task is a familiar one, then hierarchies can perform very well...Information needs, as formally expressed by the essential elements of information and information exchange requirements, are likely to be well known. Thus, it is likely that the right information is provided to the right entities at the right time...All of this changes when hierarchies are faced with unfamiliar tasks or need to perform in an unfamiliar situation [1:p. 219].

"The goal is not to be able to perform well in a particular mission in a particular situation, but to create an organization that is agile [1:p. 180]." This research takes a bottom-up approach to suggesting a an agile organizational topology.

2.3.2 Human/Organizational Aspects of NCO Theory. The DoD is using NCO to shape the future force, publishing a series of Joint Concepts that address NCO implementation over the next 10 to 20 years. These concepts emphasize both the human and technical aspects of NCO: “Net-Centric capabilities focus directly on human interaction through knowledge sharing enabled by the dramatic advances in information technology [20:p. 1].” The Network-Centric Environment Joint Functional Concept (NCE-JFC) best describes the roles and responsibilities of individuals and suborganizations operating in such an environment:

> Individuals in the Net-Centric Environment have decision rights and responsibilities and will be empowered and enabled to act freely in making decisions. They have the responsibility to make those decisions within the context of command intent and to share situation understanding across the Joint Force and its mission partners. These rights and responsibilities apply to both the formal command and control process and to less formal collaborative decision structures. Decisions in the Net-Centric Environment are heavily influenced by dynamic, self-defining patterns of collaboration [20:p. 15].

This excerpt points to three seminal concepts that spawned this research effort. The first is that individuals in the net-centric environment have decision-making responsibility and must collaborate to fulfill that responsibility. Second, individuals and suborganizations must be tied to a command and control structure from which they receive “command intent” and through which they pass “situation understanding” to the rest of the network. Finally, the relationships among individuals in the net-centric environment are “dynamic and self-defining.”

The individuals and suborganizations are called Communities of Interest (COI). A COI “consists of a group of people [individuals or suborganizations] who interact [or collaborate] for a common purpose and/or interests, typically because of interdependent tasks [21:p. 15].” Collaboration is a key construct in this research. Collaboration can be almost anything that net-centric entities share: information, resources, personnel, etc. A collaboration is anything that is useful in making a decision, solving a problem, or performing a task. It is the lifeblood of the agile organization; it is what flows through the organization.

COIs relate to each other through collaborations and are the building blocks of NCO organizations. How they fit together is the subject of much study (including this research) and debate. While a great deal of work is being done on the problem, specific solutions are not immediately forthcoming. The NCO Joint Concepts along with documents such as the Network Centric Operations Conceptual Framework (NCO-CF) suggest directions for study and experimentation [34]. They suggest concepts, hypotheses, and high-level metrics that researchers and developers might use to contribute to the body of knowledge. This research effort builds not only upon the high-level concepts but other work that suggests more specific structures and metrics.

One such structure is the small world network where tightly clustered communities are connected by "weak ties" to other tightly clustered communities leading to short geodesic distances (number of hops) between any two actors in the network. Small world networks occur frequently in nature, and are thought to provide high flexibility and agility. Small world networks have received attention from NCO theorists for several reasons. First and foremost, they may facilitate both the control structure and operational agility sought in today's uncertain environment [4:p. 173]. Next, they are characteristic of naturally-occurring social networks; people naturally organize themselves into small world networks. Finally, they do not depend entirely on chance as do other types of networks [4]. Agile, rule-based organizations can, theoretically, be designed using the small-world construct. Returning to the NIMS domain, Compagnoni writes,

> Perhaps the use of hierarchies is sufficient at the federal and state levels because of the stable environment, but crisis conditions at the local level should lead us to consider employing an all-channel network to improve organizational agility and resilience [16:p. 66].

This thought, that an organizational topology can simultaneously provide control structure and operational agility, forms a pillar of this research.

Watts provides the definitive treatment of small worlds networks. He points out that the most significant problem in studying social networks empirically is in defining what constitutes a relationship or the social "distance" between two entities [67:p. 22].

Watts does not therefore focus on an empirical study of real networks, but a theoretical study of network constructs. He simplifies the problem by classifying graphs into two broad categories: relational and spatial. Watts creates relational graphs by assuming that network nodes are either connected or they are not; entities either know each other or they do not. This allows global-level relationships that are independent of node attributes, the strength of a relationship, ability to communicate, etc. Moreover, in Watts' model these relationships are random. He randomly rewires graph edges to create global links between nodes. Watts explains that the "dual concept of two length scales (local and global) coexisting in a graph is the key to explanations of length and clustering phenomena [67:p. 96]." Surprisingly the small world effect presents itself when only a few such global edges (less than 10 percent) are created [67].

Spatial graphs, however, rely on distance metrics. Nodes are related in some way, and the strength of these relationships is significant. The easiest concept to understand and the one used in this research is geographical distance. If two entities are geographically close to each other, they are connected. Watts explains that for spatial graphs

> edges can never connect verticies from distant parts of the graph until that length scale is made sufficiently large that it encompasses the entire graph. By that stage, the graph is no longer clustered [67:p. 96].

In order for geodesic distance to be reduced, longer connections must be made; when longer connections are made, clustering increases, but so does network density. The graph becomes not a network of small interconnected clusters, but one big cluster. The global topology takes on the characteristics of the local topology, and instead of having tight communities connected by weak ties, the network becomes one big tightly clustered community. Such an organization is neither structured nor agile, which are the goals of net-centric operations. This discussion points to two network characteristic metrics that are important in this research: clustering coefficient and density.

In summary, relational graphs can exhibit small world characteristics; spatial graphs cannot. The types of networks discussed in this research exist in geographical space. They are spatial graphs. Despite this apparent roadblock, the small world concept is useful in the net-centric discussion. The characteristics of the small world network are tight clustering and short geodesic distance. The idea of net-centric operations is to form COIs (clusters) using "dynamic, self-defining patterns of collaboration" linked to a command and control network, which provides global links to the rest of the network thereby reducing geodesic distance. The models studied in this research are built upon these concepts.

2.3.3 Metrics. The idea of viewing organizations as networks is now commonplace. The discussion heretofor has only scratched the surface of the enormous body of literature on this subject. Consensus is, however, lacking on how to measure the "network-ness" of an organization, and what constitues "goodness" and "badness" in network topologies. Watts proposes distance and clustering coefficient to identify and describe relational small world networks. These metrics prove useful in this research, but do not show the complete the picture.

NCO theorists propose a model of the net-centric environment (Figure 2.5) that proceeds from a "force" (read organization) embedded in an environment to its "degree of effectiveness." Processes are conducted in the physical, information, cognitive, and social domains, which compliments and decomposes the previously discussed knowledge/technology duality. The following definitions are given for the four domains:

- Physical Domain: where effects take place and where other supporting infrastructure and information systems exist
- Information Domain: where information is created, manipulated, and shared
- Cognitive Domain: where perceptions, awareness, beliefs, and values reside and where, as a result of sensemaking, decisions are made
- Social Domain: set of interactions between and among force entities [34:p. 56]

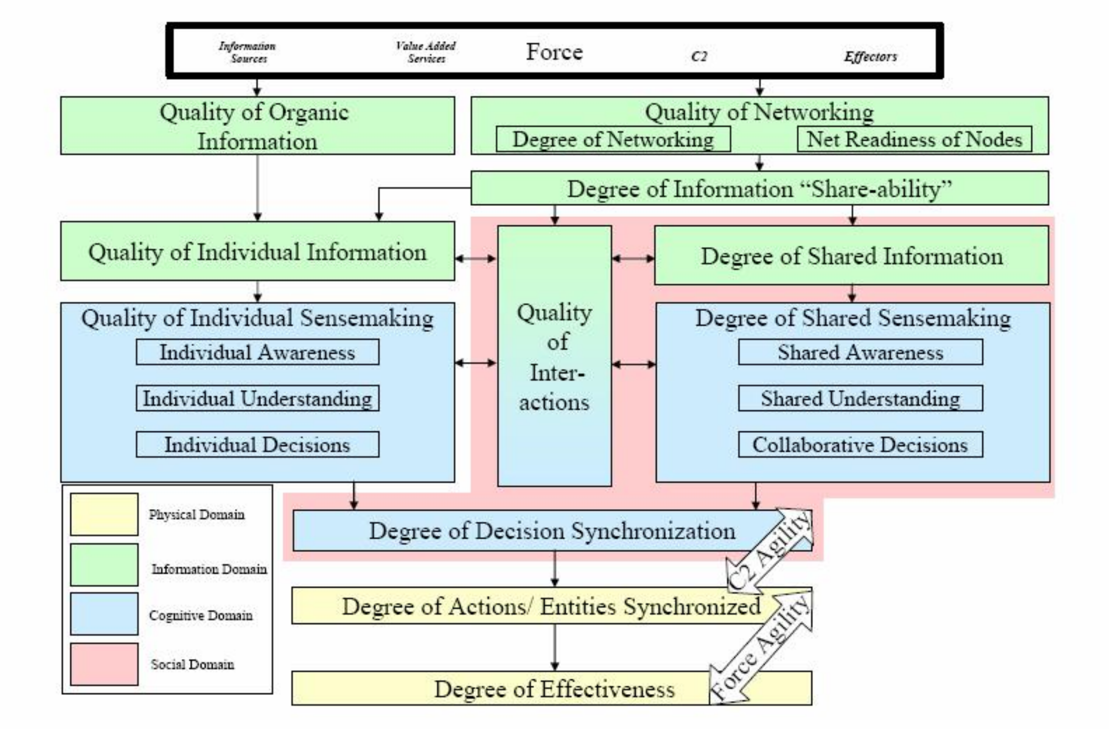


Figure 2.5: The NCO Conceptual Framework [34:p. 58]

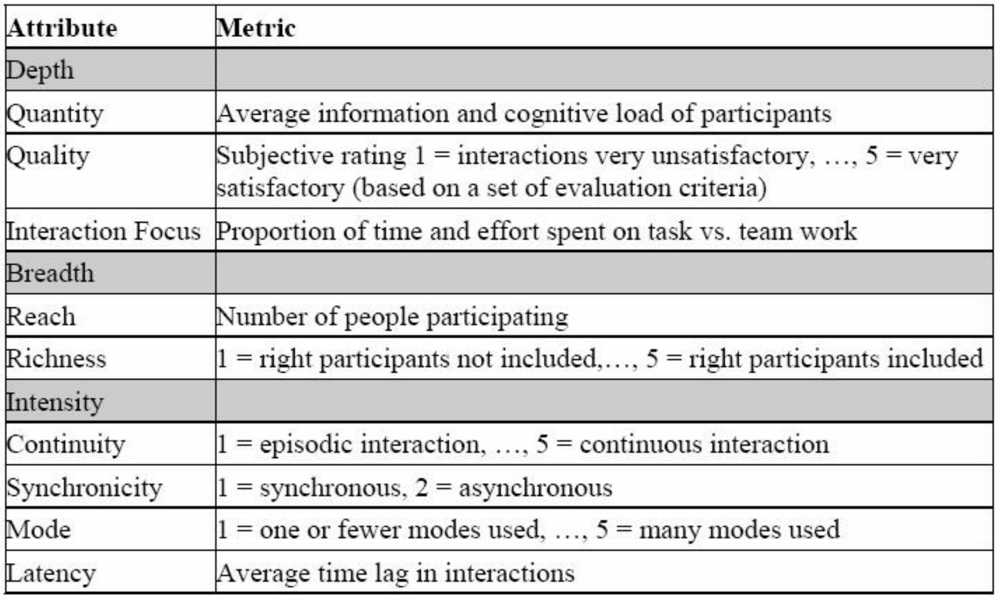
The central element in Figure 2.5, *Quality of Interactions*, contains the links that bind individuals to the rest of the network. This is where network entities collaborate. The NCO-CF proposes four top-level attributes of interactions:

- Depth: measures that describe the nature of the substance of interactions
- Breadth: measures that describe the force entities that interact
- Intensity: measures that describe the pace and completeness of interactions
- Agility: measures that describe the robustness, resilience, flexibility, responsiveness, innovativeness, and adaptability of interactions [34:p. 127]

The NCO-CF further proposes subattributes and metrics to evaluate them:

One can see that these metrics are very high-level and quite subjective. Moreover, the NCO-CF does not propose methodologies for collecting them. Finally, the metrics themselves imply survey data collected from individuals involved in "live fire"

Table 2.3: Quality of Interactions: Attributes and Metrics [34:p. 128]



Attribute	Metric
Depth	
Quantity	Average information and cognitive load of participants
Quality	Subjective rating 1 = interactions very unsatisfactory, …, 5 = very satisfactory (based on a set of evaluation criteria)
Interaction Focus	Proportion of time and effort spent on task vs. team work
Breadth	
Reach	Number of people participating
Richness	1 = right participants not included,…, 5 = right participants included
Intensity	
Continuity	1 = episodic interaction, …, 5 = continuous interaction
Synchronicity	1 = synchronous, 2 = asynchronous
Mode	1 = one or fewer modes used, …, 5 = many modes used
Latency	Average time lag in interactions

experiments. In short, while the metrics proposed in the NCO-CF point the way for further research, they have limited utility in their own right. This is actually an achievement of the NCO-CF as its purpose is not to propose a standard set of metrics, but a framework of high-level metrics upon which researchers can build.

Wong-Jiru extends the NCO-CF by applying social networking theory metrics to a multi-layer network model [72]. She uses a set of 12 metrics defined by Hanneman [36] to develop a net-centric value for each layer of her model. These N_{layer} values are rolled up into a total net-centric score for the system. Her goal is to show how a failure or perturbation at a lower level of the model affects mission performance at the process layer where people perform their work. Significantly, she explains how Hanneman's metrics might apply to the high-level NCO-CF metrics. Her ideas are crucial to this research where the *Depth* and *Breath* NCO-CF attributes are extended using Hanneman's social networking metrics of distance, clustering coefficient (also proposed by Watts), density, and centrality.

The importance of distance and clustering coefficient to this research have already been discussed. Density describes is the ratio of the number of edges present in a graph to the number of edges that could exist in a graph. When clustering coefficient is compared to density in a spatial graph one can determine whether high clustering is due to local or global edge effects. Centrality is used to measure the effectiveness of the command and control system that provides the global connectivity among the response nodes in the model. Hanneman explains that as organizations are increasingly viewed as networks, the position of an entity with respect to all other entities defines its opportunities and limitations, or its power. A highly central entity has more power [36]. Particularly germane to this research is the idea of betweenness centrality where an entity is on the shortest geodesic path between two other actors or it is not. The more of these paths an entity is on, the more power it has. Hanneman also provides a metric that indicates the betweenness centrality for the entire graph. The alogorithms for calculating these metrics are given in Chapter Three of this research.

2.4 Summary

The events of 9/11 and Hurricane Katrina highlight shortcomings in the National Incident Management System. A common problem identified throughout the literature is lack of interoperable communications systems. A review of public safety communications systems shows a myriad of interoperable and non-interoperable systems in use today and various attempts to patch these systems together. The approach taken in this research is to use a top-down approach to identify capability gaps and propose material solutions to fill those gaps. The proposed physical solution provides ubiquitous communications, which are a necessary but not sufficient condition for an effective disaster response system. NCO concepts are used to suggest an organizational structure that facilitates effective patterns of collaboration and improved organizational effectiveness.

III. Methodology

3.1 Overview

3.1.1 Problem. This research addresses the problem of organizational performance in unforeseen, unpredicatble, and/or dynamic situations. The context used is the National Incident Management System response to major disasters (e.g. Hurricane Katrina) or incidents of national significance (e.g. 9/11).

3.1.2 Goals. This research effort has the following goals:

1. Evaluate technological solutions that provide fully interoperable communications and enable the collaborations described herein.
2. Evaluate the effect of collaboration while maintaining the integrity of a hierarchical command and control structure in a disaster response context.

3.2 Physical Solution Evaluation Methodology

The purpose of this section is to detail the methods in which the functional need of rapidly deployable, interoperable communications systems develops into a proposed RDNS solution. Furthermore, it evaluates the effects of collaboration in a hierarchical command and control structure.

3.2.1 Rapid Network Deployment System Concept of Operations. The Rapid Network Deployment System (RNDS) concept consists of a temporary communications infrastructure for emergency response personnel, which can be established within a short period of time following a disaster. In the first hours following an incident, public safety personnel disperse into the community to provide aid to citizens as needed. At the same time, designated personnel utilize one or more pre-packaged and pre-configured Rapid Network Deployment Kits (RNDK) to establish jurisdictional level wireless access nodes. Each kit contains all the equipment necessary to set up and power a medium-range wireless base station. Also, the kits are relatively low cost to purchase and can be maintained by local public safety officials until needed. Once deployed, the RNDK provides communications links between emergency responders and establishes a backhaul connection to an internet point of presence.

3.3 Physical Solution Evaluation Methodology

If the issues of multi-agency incident response and rapid network deployment are allowed to be paralleled with issues encountered in joint military operations, the tools and concepts used in the DoD system development process can be referenced. A comparison of these two arenas is both reasonable and logical in that the overarching capability of the DoDs future vision regarding information sharing in joint environments contains many of the same aspects as the DHS's vision of operations in multi-agency environments. For example, the DoDs Joint Vision 2020 addresses a faster, more lethal, and more precise Armed Force in 2020 [17]. This statement applies directly to DHS in regards to incident response and management. If emergency management agencies are to be faster, more effective, and more efficient in the future, they must continue to invest in and develop new capabilities. Joint Vision 2020 also suggests that superior information is the key to military victory. This holds true in large-scale disasters in that superior information leads to successful response, management, and recovery from an incident. It has been shown that net-centric operations, with interoperability, agility, scalability, and rapid deployment as key enablers, are a primary objective of the DoD. The knowledge management modeling of this thesis demonstrates how net-centric operations improve the overall effectiveness of incident responders. Therefore, these same key enablers of net-centricity can be used as driving forces for our solutions development. The methodology for the Rapid Network Deployment System (RNDS) begins with a discussion of the DoDs Joint Functional Concept documents and how they provide a traceable link to an overarching capability during a system development process. Since the idea of a hastily-formed, interoperable communications network relates to tenants associated with net-centric environments, a parallel may be drawn between the DoD and the DHS views of the topic. Therefore, the links found in references provides valuable insights into tasks and capabilities needed to be accomplished with the proposed RNDS.

3.3.1 Methodology Background. The DoD uses the Joint Capability Integration and Development System (JCIDS) and the DoD 5000 series of instructions as the primary references to new systems development. JCIDS provides the DoD with a system to identify, assess and prioritize joint military capability [12]. It uses a top-down approach to system development which is capability driven vice requirements driven. This approach aims to prevent stove-piped systems from being developed. According to S1, a concept is defined as ideas about how something might be done with resources we do not have yet. JCIDS implementation requires using joint concepts to identify and describe existing shortcomings and redundancies in

> . . . capabilities; describe effective solutions; and provide potential approaches to resolving these shortcomings [12].

The joint concepts methodology referenced in the JCIDS process is guided by various documents including Concept of Operations (CONOPS) and the Family of Joint Future Concept (FJFC). Both of these document sets receive their direction from the overall DoDs strategic guidance. CONOPS allow the joint community to alter or divest current capabilities to fulfill a need in the near future. It provides a means to substantiate current programs. The FJFC is used to underpin acquisition decisions leading to new capabilities beyond five years. It is hierarchical in nature and provides a deliberate and iterative process for capability assessment. All new capability requirements ..must relate directly to the capabilities identified through the FJFC [12]. The FJFC consists of the Capstone Concept for Joint Operations (CCJO), Joint Operating Concept (JOC), Joint Functional Concept (JFC), and Joint Integrating Concept (JIC). Each one of these documents provides a varying level of specificity regarding defining a capability requirement. The CCJO provides a broad overview of how joint forces are expected operate in the future. It is informed directly from strategic guidance. The CCJO attempts to transform its strategic guidance into concept and policy applicable globally across the DoD. The JOC is the next level down from the CCJO. It addresses more defined areas of military operations, thus scoping the CCJO into categories. The JOC identifies challenges faced by the operational commanders and attempts to address the capabilities needed to overcome them. The JOC is divided into four major conceptual areas as seen in Figure 3.1. The JFC is the next level of abstraction after the JOC. Whereas the JOCs focus is at the operational level, the JFCs focus is at the functional level. JFCs broadly describe functional capabilities relevant to a specific problem, which are needed to support the concepts in the JOC. They are divided into eight areas of focus. JICs are the lower level concepts and contain a narrower perspective of the topic. They describe specific operations, tasks, or functions required to implement the concepts contained in the operational level JOCs and the functional level JFCs. In short, JICs are a statement of how something might be done; in particular, it states how we would like to do that thing in the future [38].

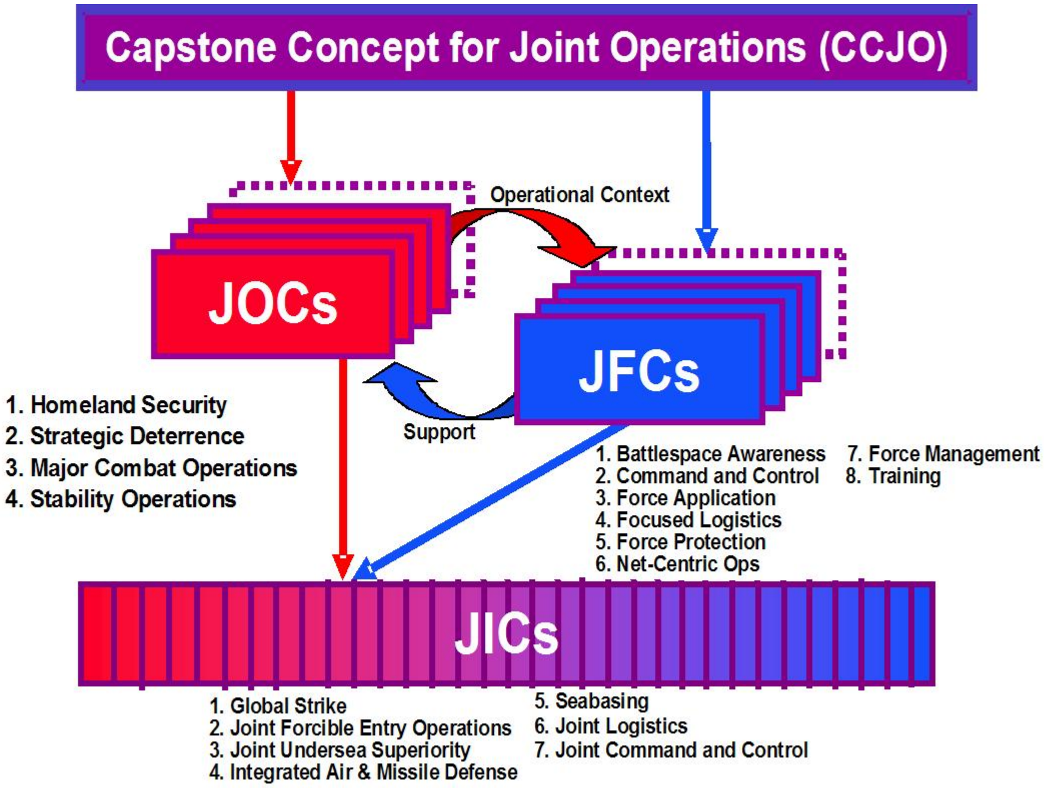


Figure 3.1: Family of Joint Functional Concepts

The concept documents are used as references and guidance to conduct further analysis into the JCIDS process. They also lead to the creation of a Joint Capability Document (JCD). The JCD is used to provide many things, among them being a traceable link between a capability being accessed and the tasks associated with it.

3.3.1.1 Approach to Solution. One of the hypothesis of this thesis stated that a temporary, hastily formed, communication network for first responders could be realized utilizing only commercial-off-the-shelf (COTS) 802.11, and 802.16 technologies. As mentioned earlier, DHS shares similar communications problems as the military. However, the authors believe that the DoDs approach for analyzing system solutions represents a more solid and systematic methodology. With regards to determining a traceable link between capabilities and associated tasks to be performed, the joint concept documents are more formalized references than anything found in the civil sector. Therefore, the hypothesis of an 802.11and 802.16 solution was subjected to the traceability process of the JCD in order to attempt to discover its overall effectiveness at performing specific task to fulfill the overarching capability of providing a hastily deployable, interoperable communication network for first responders. First, applicable DoDs joint concepts were compared with concepts of the DHS in order to demonstrate their similarity. This required a review of applicable documents from the two arenas. Principle documents used were the FJFC, NIMS, and the SAFECOM SoR. The end result was a traceable path from overall high level-capabilities to the lower level tasks associated with them. Next, the tasks needed to enable our desired capability were defined in accordance with the DoDs and the DHSs ideology on the subject. Finally, the hypothesized solution was assessed to determine its effectiveness in fulfilling the discovered tasks. This assessment included documenting technical specifications and features of each sub-system of the RNDS proposal and determining their overall ability to meet system requirements.

3.3.2 Physical Solution Methodology Scope. The JCIDS development process is referenced in order to establish parallel traceable links between the DoDs view of a joint communications environment and that of the DHS. It was not the intent of the authors to perform a full JCIDS analysis or a Capability Based Assessment (CBA). Rather, the goal was to utilize a proven DoD process and the overall format to aid in the discovery of the tasks involved in realizing a hastily formed and interoperable communications network.

3.4 Knowledge Management Methodology

Results of the physical solution analysis reveal that ubiquitous communications are possible using technologies described in Chapter Four of this thesis. The question of how to achieve *effective communications* remains. This section describes an approach to answering that question using graph theory and social network analysis techniques.

3.4.1 System Description. The system under consideration is the ICS, the primary system used in the United States and Canada for the command, control, and coordination of resources during an incident. Components of the ICS include the organization, facilities, infrastructure, and resources used to respond to a major disaster or incident of national significance. This research considers the organizational component.

As discussed in Chapter Two of this thesis, an organization's structure partly determines its performance characteristics. The ICS defines the relationships, or social links, that allow organizational entities to exchange information, or collaborate; the ICS produces a social network. The ICS also produces a communications network from its collection of technical components that enable these collaborations. The structure, or topology, of these two networks together determine the degree of collaboration among organizational entities and, theoretically, the performance of the system.

A distinction is made between the command and control structure of the ICS and the "edge" of the ICS where first responders interact with the environment. The command and control topology, consistent with the ICS, is hierachical; the topology created by enabling response nodes to collaborate, or the *response topology*, is the subject of this research. Since the "as-is" system, the ICS, has a hierarchical topology, the methodology begins with the assumption that response nodes do not collaborate with each other; they collaborate only with their assigned $C2$ node. The other two topologies, complete and hybrid, each define a different manner in which response nodes collaborate with each other. Of these three response topologies, one is analytically found to be most desirable. This topology is then applied to a complete ICS model and tested using computer simulation.

3.4.2 Evaluation Technique. The difference between the three topologies is the method of collaboration. In the hierarchical topology, response nodes cannot collaborate with each other, while each response node collaborates with all other response nodes and the $C2$ node in the complete topology. The hierarchy and the complete topologies are opposites. The hybrid topology is constructed by allowing some response nodes to collaborate with each other according to an algorithm described in Chapter Four of this thesis.

Encarta defines collaboration as “the act of working together with one or more people to achieve something [52].” All nodes in the system, $C2$ and response, have both the ability and the need to collaborate. The ability/need duality of collaboration captures the dynamics of interpersonal communication. If either party in an interaction is distracted or otherwise occupied, effective communication does not occur. Information may be incorrectly conveyed, misunderstood, or just lost. In this research the idea of communication is extended to collaboration under the assumption that if two entities collaborate effectively, they must communicate effectively. The number of collaborations, communications, interactions, relationships, etc., and the amount of information one can process before misunderstanding or completely missing something is the subject of much study in the field of cognitive psychology.

The concept of *channel capacity* introduced in Miller’s seminal work on cognitive psychology [48] is the basis for quantifying collaboration in this research. The title, *The Magical Number Seven, Plus or Minus Two* hints at the content of the paper. Humans can only remember about seven (plus or minus two) pieces of information be they digits in a telephone number or names of people met at a cocktail party. Miller points out that this number varies depending on context, but makes the point that humans have a limited capacity to process information beyond which errors are made and/or information is lost. Without delving into the field of cognitive psychology or performing a work domain analysis of the emergency response field, an attempt is made to quantify collaboration in the context of this research by using response nodes as the baseline for collaboration ability.

Let response nodes have a collaboration need of one unit and a collaboration ability of one unit. This means a response node can provide one unit of collaboration to its neighbors and needs one unit of collaboration from its neighbors to effectively serve its purpose. Similarly, let a $C2$ node's ability/need to collaborate be five or less as this is commensurate with its span of control as defined by the NIMS. If a $C2$ node has five or fewer subordinate response nodes, it provides each of them with one unit of collaboration, and their needs are met. Conversely, the $C2$ node receives one unit of collaboration from each of its subordinate response nodes (five or less), and its collaboration needs are met. If a $C2$ node has fewer than five subordinate response nodes, there are, by assumption, fewer than five incidents in that $C2$ node's jurisdiction. Less information is in existence, so the $C2$ node needs less collaboration. Conversely, a response node handling a single incident still needs its full measure of collaboration whether other incidents exist or not.

This balanced collaboration dynamic exists in hierachical systems, represented graphically in Figure 3.2, under circumstances for which they are designed. Figure 3.3, however, shows an overload situation where each $C2$ node's ability to collaborate is divided among more than five response nodes. Its span of control is exceeded. Each response node now receives less than one unit of collaboration from its associated $C2$ node. Conversely, if, as this model assumes, each response node also provides one unit of collaboration, its associated $C2$ node receives too much collaboration. Overall, the system

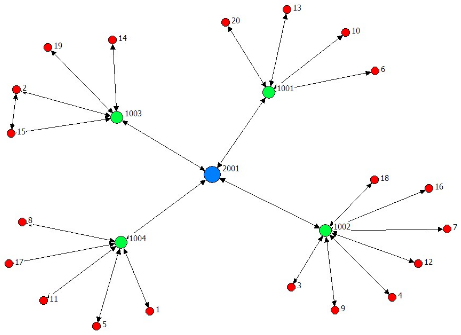


Figure 3.2: Balanced collaboration in hierarchical system

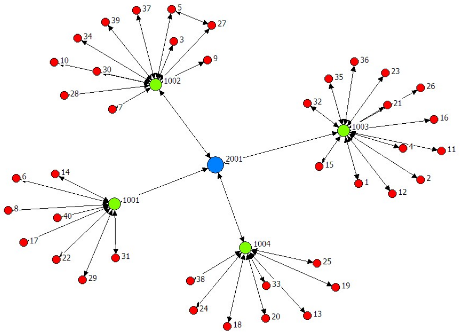


Figure 3.3: Overloaded Hierarchy

as a whole is less effective. This research proposes a solution to this dilemma by allowing response nodes to collaborate with each other thus balancing the system.

3.4.3 Graph Theory Analysis.

The purpose of using graph theory is to propose an optimal response topology, which is then integrated into a complete command and control system in the simulation study described below. This analysis therefore considers only one $C2$ node along with its associated response nodes. The graph theory study has a one-factor (topology), three-level (hierarchy, complete, hybrid) experimental design where nodes are the workload on the system and the system response is its abiltiy to accommodate the nodes based on the metric *collaboration capacity*.

The organizational topology described in the NIMS is a hierarchy where each subordinate formally collaborates only with its superior. At the lowest level, the star graph, Figure 3.4, represents this situation.

In terms of collaboration, a star topology is balanced until the $C2$ node's span of control is exceeded at which point the $C2$ node is overloaded and the response nodes are underserved. This analysis proposes a method for balancing the system by allowing response nodes to collaborate. Collaboration rules among response nodes are varied to create three different response topologies: the hierarchical topology, the complete topology (or complete graph), and the hybrid topology. All of these topologies are based on the star substrate. The metric used to compare these three levels of topology

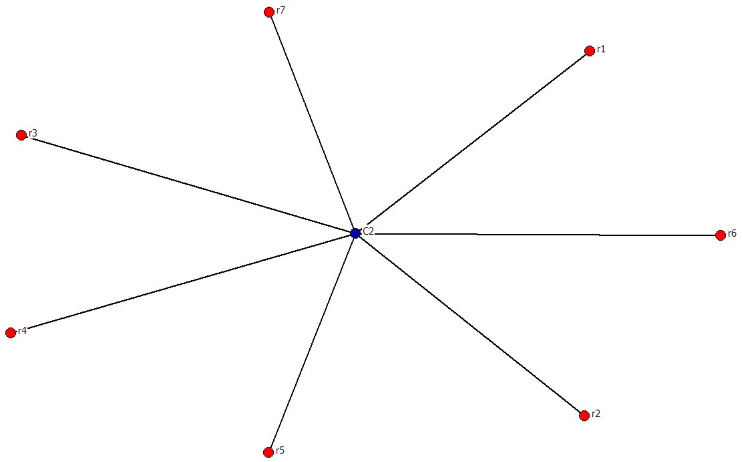


Figure 3.4: Star Topology

is *system collaboration capacity*, $CC(G)$, where G is the graph of the entire system: the $C2$ node, the response nodes, and the edges between them. First, a topology-independent relationship between number of response nodes, n, and maximum system collaboration capacity, $CC(G)_{max}$ is developed, then the three competing topologies are evaluated to determine whether or not they achieve $CC(G)_{max}$.

Let the nodes, $C2$ and response, represent the load on the system. The system response is the capacity to meet the collaboration needs of the nodes. A weighted edge between two nodes represents the system's ability to meet the collaboration needs of both nodes. This model assumes that two adjacent nodes collaborate equally and that nodes cannot be overloaded. This allows the use of a weighted undirected graph for this analysis where the undirected edge between two nodes accommodates the load of both nodes. System collaboration capacity, $CC(G)$, is represented mathematically by the sum of the edge weights:

$$CC(G) = \sum_{j=1}^{e} w_j \tag{3.1}$$

where w_j is the weight of the j^{th} edge and e is the number of edges in G.

Coincident with its span of control, the $C2$ node has a load of five collaboration units ($l(C^2) = 5$), where $l(v)$ is the load on the system produced by node v. Each response node has a load of one collaboration unit ($l(r_i) = 1$). A node's load is accommodated by the edges incident to it where the number of incident edges is the node's *degree*, $d(v)$. An edge's weight is determined by the load and degree of its incident nodes such that

$$w_j = \frac{l(v)}{d(v)} \tag{3.2}$$

For example, if a $C2$ node has five response node, its degree is five and $d(C^2) = 5$. Since a $C2$ node's load is also five ($l(C^2) = 5$), the the weight of each edge is one.

This model assumes that load is accommodated to the maximum extent possible by the edges between response nodes and the $C2$ node. This assumption captures the idea that responders collaborate preferentially with the command and control system in a hierarchical organization. This model further assumes that nodes cannot be overloaded, so the sum of the edge weights incident to $C2$ cannot exceed five collaboration units nor can the sum of the edge weights incident to a response node exceed one collaboration unit.

When a response node is added to the system, an edge is created between it and $C2$. When there are five or fewer response nodes, the weight of each edge is one. If there are more than five response nodes adjacent to $C2$, by assumption it collaborates equally among them, but less effectively. Since the model assumes nodes cannot be overloaded, edges between response nodes and $C2$ are weighted as follows:

$$w_{C^2,r_i} = \begin{cases} 1 & n \le l(C^2) \\ \frac{l(C^2)}{n} & n > l(C^2) \end{cases} \tag{3.3}$$

When $n \le l(C^2)$ the system is balanced. As n increases above $l(C^2)$, the edge weights are less than one. While $C2$'s load is accommodated, each response node has excess load, $l_e(r_i)$, such that

$$l_e(r_i) = 1 - \frac{l(C^2)}{n} \tag{3.4}$$

To balance the system, weighted edges are created between response nodes to accommodate the excess load. These edges represent collaborations between responders. A topology-independent relationship is developed between the number of response nodes and the system collaboration capacity needed to accommodate them. To do this, it is necessary to consider only the response nodes and the edges among them, or mathematically, the graph R induced by removing $C2$ ($R = G - C^2$). The results of this treatment are presented in Chapter Four of this thesis, and suggest not only an optimal topology but additional graph theory metrics with which to evaluate simulation data.

3.4.4 Simulation Study. Simulation experiments are used to evaluate the performance of the ICS using a fixed command and control system and the hybrid edge topology embedded in a simulated 20 unit by 20 unit geographical space representing a county-level jurisdiction. Figure 3.2 above shows a sample topology with the fixed command and control nodes surrounded by 20 randomly located response nodes [numbers 1 - 20 (in red)]. The model space for which a $C2$ node is responsible is its *jurisdiction*. Node number 2001 is the highest level $C2$ node representing a county-level EOC. Nodes 1001 - 1004 are $C2$ nodes responsible for a 10 unit by 10 unit space representing municipal EOCs within the county. Response nodes that represent the first responders are the workload on the system.

All nodes, $C2$ and response, have both the ability and the need to collaborate. An edge between two nodes represents a collaboration. Collaborations are established based on the response node parameter *location*, which is randomly assigned to each response node and determines its relationship to the command and control system and to other response nodes. A response node has a location within a jurisdiction, so a collaboration is established between that response node and the $C2$ node responsible for the jurisdiction in which it is located.

In the simulation model the amount of collaboration a node gives to or receives from its neighbors is quantified using directed edge weights. Using Figure 3.5 as an example, the star node has two neighbors; its degree is two. It provides each of its neighbors, the square nodes, with an equal amount of collaboration, represented by the directed edges from the star to the squares. Assuming the star is a response node with a collaboration ability of one, the weight of each of these outwardly directed edges is one half. Similarly, each square node provides each of its neighbors with an equal amount of collaboration. In this case, however, the square nodes have three neighbors, so the weight of each outwardly directed edge is one third. Since each square node only provides one third of a unit of collaboration to the star node, the latter only receives two thirds of a unit of collaboration. The square nodes, on the other hand, are the victims of "information overload" since they each receive a total of two and a half units of collaboration. The star node is underserved; the square nodes are overloaded. The metric used to quantify a node's performance is its weighted in-degree, d^+_{tot}, or the sum of the weighted inwardly-directed edges incident to it. d^+_{tot} represents the amount of collaboration a node receives from its neighbors, which is a measure of effectiveness in this research.

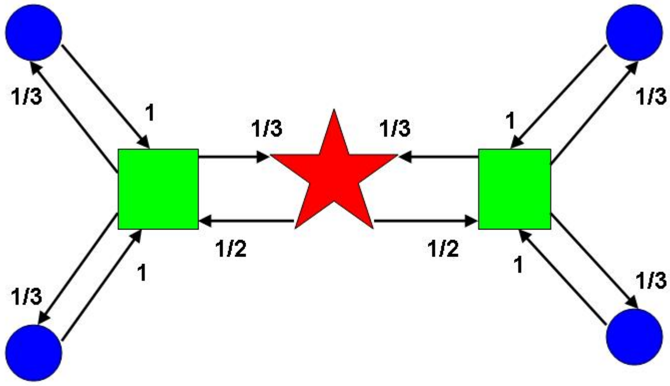


Figure 3.5: Weighted Edge Calculations

This discussion points to the first experimental factor in this research: the number of nodes in the system. The set of simulation experiments begins by randomly assigning 20 response nodes to locations within the model space. Simulation runs are also conducted using 40, 60, and 80 response nodes. Using a purely hierarchical model where no collaborations exist between response nodes, system performance is expected to be inversely proportional to the number of response nodes in the system. The governing hypothesis of this portion of the research is that by allowing response nodes to collaborate with each other, the $C2$ system is less likely to be overloaded, their collaboration needs are more likely to be met, and the system as a whole is more effective. An algorithm for creating collaborations among response nodes is now proposed.

It is assumed that in a disaster response situation responders that are in close geographical proximity may have the need to collaborate. *Closeness* is captured in the second experimental factor, *range*, R. If the distance between two response nodes is less than or equal to the range level, a collaboration is established between them. Range levels tested are 0, 1, 3, 5, 10, and 15 units whereas the simulation space is 20 units by 20 units with each 1000-level jurisdiction measuring 10 units by 10 units. Range zero represents the hierarchical topology where response nodes only collaborate with their associated $C2$ node (unless they are randomly placed in the same location by the model). By comparing Figure 3.6 with Figure 3.3 above one can see that by changing range from zero to five individual nodes become much more interconnected and the graph as a whole loses much of its hierarchical structure. The questions to be answered are:

- How much interconnection (collaboration) is enough?
- How much structural loss is too much?

The final factor is collaboration preference, P, which captures the difference between a system with a robust command and control system and a more ad-hoc network. Collaborations between response nodes and their assigned $C2$ node are either given preference or they are not. P is therefore a Boolean variable tested using two seperate model versions. In the integrated version the edge between r_i and $C2$ is weighted such that the $C2$ node always receives its full measure of collaboration. Response nodes then share

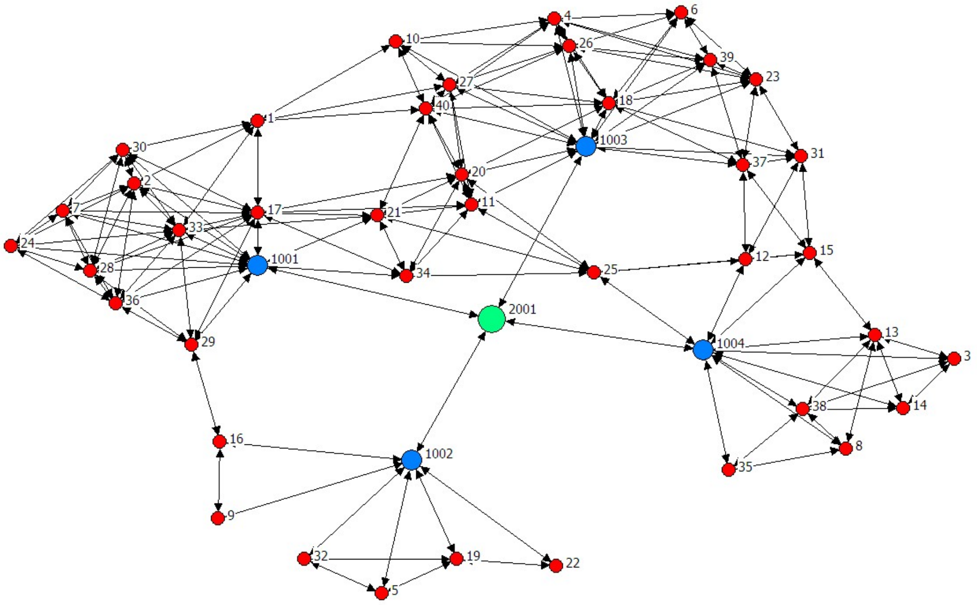


Figure 3.6: Loss of hierarchical control. Hybrid Topology: 20 Nodes, Range = 5.

their remaining collaboration with each other. This model version is consistent with the mathematical model described above. In the ad-hoc variation, the weighted out-degree of a response node is divided evenly among its neighbors, including $C2$.

In summary, the simulation study is a three-factor simulation experiment. The factors are number of response nodes, n; range, R; and collaboration preference, P. System response is categorized into network characteristics and node effectiveness. The network characteristics are measured using the social networking software UCINet; specific network metrics are described below. Node effectiveness is measured using the average weighted in-degree for a given network iteration also described below.

3.4.4.1 Network Characteristics. The simulated disaster response environment is first evaluated using the social networking metrics *average distance*, *density*, *clustering coefficient*, and *betweenness centrality*. The social networking software UCINet is used to glean these metrics from the network models in the form of adjacency matrices created in Microsoft Excel as described in Appendix B. These metrics are defined as follows [9]:

- Average Distance: The length of a path is the number of edges it contains. The distance between two nodes is the length of the shortest path. The average distance is reported in this research.
- Density: The density of a binary network is the total number of ties divided by the total number of possible ties.
- Clustering Coefficient: The clustering coefficient of a node is the density of its neighborhood. A node's *neighborhood* is the set of nodes adjacent to it. The overall clustering coefficient is the mean of the clustering coefficient of all the nodes.
- Betweenness Centrality: Betweenness centrality measures information control. Let bjk be the proportion of all geodesics linking vertex j and vertex k which pass through vertex i. The betweenness of vertex i is the sum of all bjk where j and k are distinct [36]. The routine also calculates the betweenness centrality index (reported in this research) based on these data.

A limitation discovered during network response analysis is that UCINet is unable to analyse weighted adjacency matrices when they are in decimal form. The authors were unable to convert the models without making material changes thus jeopardizing validity. Unweighted adjacency matrices, where two nodes are either connected or not, were therefore used by necessity. The effect of this limitation is that this data cannot be compared quantitatively with the metrics that follow. Significant qualitative information is gleaned from this analysis, however, that is used to limit the scope of the numerical analysis that follows. Briefly, the network analysis shows that collaborations beyond a range of five units creates undesireable network characteristics. Specifically, density increases to the point where collaborative effects are global, not local. In other words, beyond $R = 5$, the system becomes one large cluster instead of four smaller ones. This has the effect of nullifying the effectiveness of the command and control system as indicated by the betweenness centrality. These results are described in detail in Chapter Four of this research.

3.4.4.2 Node Effectiveness. The simulation model calculates the total weighted in-degree (d^+_{tot}) of response and $C2$ nodes. d^+_{tot} is the amount of collaboration a node can receive from its neighbors. Ideally, d^+_{tot} of any reponse node is one; d^+_{tot} of any $C2$ node is five. Since d^+_{tot} of any node is dependent upon the weighted out-degree of its neighboring nodes, d^+_{tot} is not an independent variable. Hanneman points out that network data are different from conventional data in that networks studies evaluate the interactions among actors, not their attributes [36]. Instead of examining individual actors, a network must be viewed as a sample from the population of all possible networks. The metric used in this research to measure the effectiveness of a sample network is the average weighted in-degree, D^+_{avg}, which is the mean of all d^+_{tot} for a sample network:

$$D^+_{avg} = \frac{1}{n}\sum_{i=1}^{n} d^+_{tot_i} \tag{3.5}$$

D^+_{avg} is calculated for the response nodes in all cases. For the weighted model where collaborations between response nodes and $C2$ are preferentially weighted. D^+_{avg} is unnecessary for the $C2$ nodes since they are never underserved nor overloaded. Relating this metric to the research hypotheses:

- Hypothesis One: When span of control is not exceeded, collaborations degrade effectiveness.
  - Only the networks where $n = 20$ are considered since, on average, the $C2$ nodes have five assigned response nodes.
  - Only unweighted networks are considered since, when preferentially weighting the $C2$ nodes, edge weights between response nodes are negligible.
  - As range increases, D^+_{avg} for response nodes is expected to increase above one.
  - As range increases, D^+_{avg} for $C2$ nodes is expected to decrease below five.
  - As range increases, density and clustering coefficient should increase; betweenness Centrality should decrease.

- Hypothesis Two: When span of control is exceeded, collaborations improve effectiveness.
  - Networks where $n > 20$ are considered as they consitute systems where the span of control is exceeded. Two factors are considered in testing this hypothesis: number of response nodes and range.
  - The ad-hoc network ($P = 0$) described above is considered in this analysis to eliminate confounding.
- Hypothesis Three: When span of control is exceeded, a robust command and control system improves effectiveness over an ad-hoc system.
  - Networks where $n > 20$ are considered as they consitute systems where the span of control is exceeded. The factor considered is preference, P, a Boolean variable. When edges connecting $C2$ and response nodes are preferentially weighted, one version of the model is used; otherwise the other is used.
  - When preference is given to collaborations with the $C2$ node, D^{+}_{avg} remains close to one as range increases while D^{+}_{avg} increases above one when $P = 0$.

The hypotheses are evaluated in chapter 4 as follows:

- Hypothesis One. A scatterplot of D^{+}_{avg} versus R is constructed. The results are compared with those gleaned from the network analysis.
- Hypothesis Two:
  - Analysis of Variance (ANOVA) is conducted to determine the sensitivity of D^{+}_{avg} to n, R, and the interaction of the two.
  - Scatterplots show D^{+}_{avg} with respect to both n and R.
  - Results are compared with those gleaned from network analysis.
- Hypothesis Three:

- Results of the ANOVA performed for Hypothesis Two are used to compare the integrated with the ad-hoc networks.
- Scatterplots show D^{+}_{avg} with respect to both P and R.
- Results are compared with those gleaned from network analysis.

IV. Results and Analysis

4.1 Physical Solution Analysis Overview

This section begins the analysis of the design requirements and capabilities of a rapidly deployable public safety communications network. These tasks and requirements are generated through a review of DoD and DHS documents which trace to the overall desired capability being enabled. A proposed design solution for the system is also provided based on the discovered tasks identified in the traceability process. The major tasks of this section are summarized below. Each one has a definitive role in the discovery of the proposed solution.

- **Concept of Operations:** Provide the concept of how the RNDS is implemented to support a hastily formed, interoperable first responder communications network.
- **Capability Traceability:** Review applicable documents from the DoD and DHS in regards to net-centric operations and interoperable communications, regardless of an existing backbone infrastructure. Show the analogous relationship between the documents in order to justify the methodology used. Also, use the documents as foundations for further entry into the capability based assessment.
- **Task Analysis:** Develop tasks list from the NIMS, ICS and SoR.
- **Systems Assessment:** Assess 802.11 and 802.16 ability to perform the discovered tasks.
- **Gap Analysis:** Determine if any gaps exist between the required capability and the hypothesized solution.

4.1.1 RNDS Scenario: Provide a Hastily-Formed Communication Network.

The Rapid Network Deployment System (RNDS) concept consists of a temporary communications infrastructure for emergency response personnel, which can be established within a short period of time following a disaster. The following scenario demonstrates how the concept can be used to create a wireless network for public safety personnel. A category five hurricane has struck a coastal city and has caused widespread destruction. The disaster spans approximately 25 square miles and has damaged a major electrical distribution station, resulting in the loss of electricity throughout much of the area. In the first hours following the incident, public safety personnel disperse into the community to provide aid to citizens as needed. At the same time, designated personnel utilize one or more pre-packaged and pre-configured Rapid Network Deployment Kits (RNDK) to establish jurisdictional level wireless access nodes. Each kit contains all the equipment necessary to set up and power a medium-range wireless base station and is maintained by local public safety officials until needed. Once deployed, the RNDK provides communications links between emergency responders and establishes a backhaul connection to an internet point of presence, thus allowing users access to remote data. As public safety personnel arrive at an incident area, they communicate with one another by using WiFi enable devices with Internet Protocol (IP) support. However, it is envisioned that emergency response personnel will connect to the network via a standardized Public Safety Communications Device (PSCD). These devices provide a host of rich features, including data and IP based voice support, which enhance overall user situational awareness and allow for the implementation of net-centric organizational concepts as discussed in the knowledge management section of this thesis. Also, RNDS components utilize smart technologies to auto-configure themselves and to auto-connect to desired available networks. After authenticating to the network, public safety personnel use services such as person-to-person calls, group-calls, and calls to individuals on the public switched telephone network (PSTN). Other features include caller identification, caller location, and geographic information system (GIS) mapping overlays with public safety personnel positional data.

4.1.2 Tracing Capabilities and Associated Tasks and Requirements from DoD and DHS publications. As mentioned previously, the DoD uses the JCIDS process to provide the guidance for system development. Borrowing from the ideology contained in the FAA a review of the FJFC documents was initiated in order to provide a traceable link between the capabilities needed for a RNDS and the tasks associated with realizing the capabilities. However, because the problem was not a military problem but rather one synonymous to a military problem, comparable documents, which guide DHS, were identified and referenced for analogous correlation.

First, the applicable guidance from the DoDs perspective which led to a similar capability requirement as that of the DHS was referenced. Each of the DoD documents referenced provide a varying level of scope of the problem. Therefore, a top-down approach began the process in accordance with the levels shown in Figure 4.1.

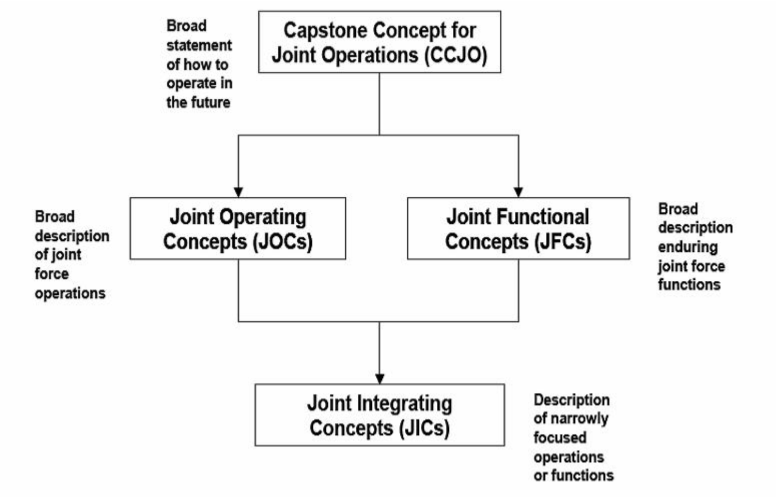

Broad statement of how to operate in the future
Capstone Concept for Joint Operations (CCJO)
Broad description of joint force operations
Joint Operating Concepts (JOCs)
Joint Functional Concepts (JFCs)
Broad description enduring joint force functions
Joint Integrating Concepts (JICs)
Description of narrowly focused operations or functions

Figure 4.1: Overview of Family of Joint Functional Concepts

4.1.2.1 Broad Statement of How to Operate in the Future. The Capstone Concept for Joint Operations (CCJO) provides the DoD with guidance on how to operate in the future. The central idea submitted in the document is:

> The joint force, in concert with other elements of national and multinational power, will conduct integrated, tempo-controlling actions in multiple domains concurrently to dominate any adversary, and help control any situation in support of strategic objectives.
>
> Primary direction from the CCJO includes the fundamental joint actions:

- *Establish, expand, and secure reach.* This action describes the ability of the joint force to access, coordinate and employ essential capabilities available inside and outside the operational area to shape an environment.
- *Identify, create, and exploit effects.* This action describes the ability of the joint force to integrate joint capabilities with those of other instruments of national power to create a desired change in the operational environment or prompt a desired action by an adversary or others.
- *Conduct integrated and interdependent actions.* Integrating joint force actions toward a common goal maximizes the complementary and reinforcing results of those actions, enhancing effectiveness and providing a bigger bang for the buck, a quality especially critical to a force operating globally with finite resources [19].

The document which most parallels the CCJO and provides a broad statement of how public safety personnel will operate in the future is the Presidential Directive for Homeland Security 5 (HSPD-5). This directive was issued by President Bush in 2003 and is used for the guidance of how homeland security is addressed in the future. It is clear that the primary underlying theme of the HSPD-5 is also coordination as evident in the following excerpt:

> The objective of the United States Government is to ensure that all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management. In these efforts, with regard to domestic incidents, the United States Government treats crisis management and consequence management as a single, integrated function, rather than as two separate functions. . . . the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The Secretary shall coordinate the Federal Government's resources utilized in response to or recovery from terrorist attacks, major disasters [54].

4.1.2.2 Broad Description of Joint Operations. Joint Operating Concepts (JOC) provide the military with a broad description of Joint Force Operation. With regards to the concept of operations of the RNDS, the Major Combat Operations (MCO) JOC is most applicable.

> This concept emphasizes the need to incorporate joint, interagency, and coalition power to achieve desired outcomes rather than to simply accomplish discrete tasks [18].

The underlying theme of the MCO JOC is:

> . . . achieve decisive conclusions to combat and set the conditions for decisive conclusion of the confrontation; use a joint, interdependent force that swiftly applies overmatching power simultaneously and sequentially, in a set of contiguous and noncontiguous operations [18];

The theme relies on effective and efficient coordination and collaboration between elements of the joint force. It involves exploiting the capabilities associated with an integrated team to totally overwhelm the enemy. The National Response Plan (NRP) parallels the MCO JOC. Its primary goal is to provide guidance for DHS personnel to:

> establish a comprehensive national, all-hazards approach to domestic incident management across a spectrum of activities including prevention, preparedness, response, and recover [26].

Key ideas expressed in the NRP which relate to the RNDS include:

- Maximize the integration of incident-related prevention, preparedness, response, and recovery activities.
- Improve coordination and integration of Federal, State, local, tribal, regional, private-sector, and nongovernmental organization partners.
- Improve incident management communications and increase situational awareness across jurisdictions and between the public and private sectors.
- Facilitate emergency mutual aid and Federal emergency support to State, local, and tribal governments.
- Facilitate Federal-to-Federal interaction and emergency support.

4.1.2.3 Broad Description of Enduring Joint Functions. The net-centric Environment JFC (NCE JFC) provides the description of joint force functions for the DoD, which would best relate to the RNDS. The central idea of the NCF JFC establishes that there are two important areas that must be brought together in order to increase mission effectiveness and efficiency.

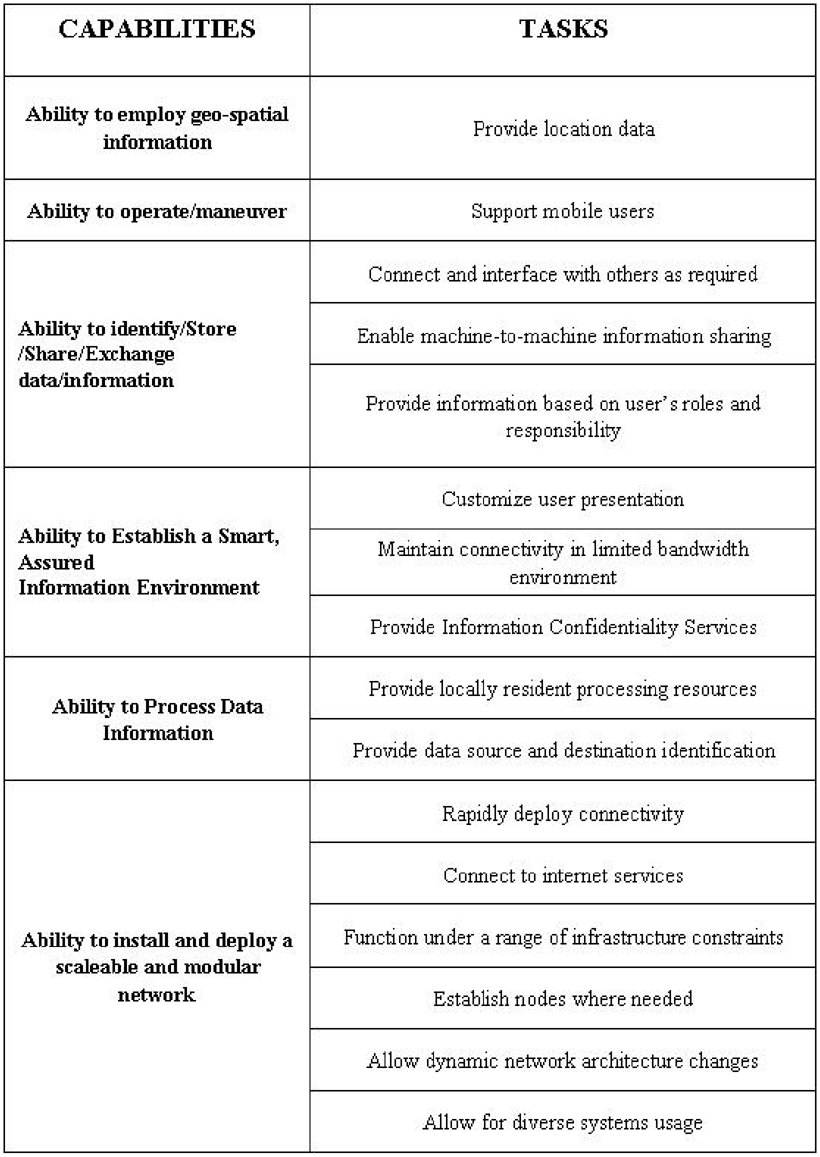
> If the Joint Force fully exploits both shared knowledge and technical connectivity, then the resulting capabilities will dramatically increase mission effectiveness and efficiency [22].

These two areas are the knowledge area and the technical area. The RNDS addresses the technical area and therefore would subscribe to tenants addressed in the NCE JFCs technical section. The NCF JFC lists multiple capabilities needed for the joint military forces to enable the net-centric environment. They are used as inputs to the net-centric Operations Environment JIC in order to develop associated tasks. The DHS has no apparent parallel document to the NCE JFC. This is because the DHS document speaks of tasks rather than capabilities. However, common ideology is found in both NIMS and the SoR.

The net-centric Operating Environment JIC (NCOE JIC) provides the description of narrowly focused operations and function for the military. It goes into further detail concerning the tasks involved in supporting the capabilities described in the NCE JFC. Table 4.1 shows a list of capabilities and tasks as identified in the NCOE JIC, which are associated with the concept of a rapidly deployable communication network for emergency responders.

SAFECOMs SoR and the NIMS give detailed descriptions of the functions and operations of the joint public safety operations. Unlike the NCOE JIC, the SoR and NIMs identify requirements vice tasks, but, tasks can be extrapolated from the requirements associated with fulfilling the RNDS concept. The following section discusses the system requirements as set forth in the SoR and is later used to expand the list of capabilities and tasks identified in the JIC. The NIMS requirements for public safety networks are not addressed independently since significant aspects are partial and redundant to the information in the SoR. Capabilities and tasks are identified from the FJFC documents

Table 4.1: Net-centric Operating Environment Joint Integrating Concepts [21]



CAPABILITIES	TASKS
Ability to employ geo-spatial information	Provide location data
Ability to operate/maneuver	Support mobile users
Ability to identify/Store /Share/Exchange data/information	Connect and interface with others as required
	Enable machine-to-machine information sharing
	Provide information based on user's roles and responsibility
Ability to Establish a Smart, Assured Information Environment	Customize user presentation
	Maintain connectivity in limited bandwidth environment
	Provide Information Confidentiality Services
Ability to Process Data Information	Provide locally resident processing resources
	Provide data source and destination identification
Ability to install and deploy a scaleable and modular network	Rapidly deploy connectivity
	Connect to internet services
	Function under a range of infrastructure constraints
	Establish nodes where needed
	Allow dynamic network architecture changes
	Allow for diverse systems usage

which relate to the RNDS concept from a DoD perspective of net-centric communications. The following sections provide an overview of the requirements for public safety communication networks as found in the SoR and gives the DHS perspective of net-centric communications.

4.1.3 Network Topology Requirements. SAFECOMs Statement of Requirements (SoR) says that the emergency responders shall establish the following networks, as required, when responding to major incidents.

- Personal Area Network (PAN): This is a very short-range network which connects devices worn by responders. Devices, such as heart rate monitors and GPS position locators use this network to communicate with the primary radio or Public Safety Communication Device (PSCD).
- Incident Area Network (IAN): This is a local area network established in the immediate vicinity of an incident. It is the primary network through which responders communicate. The short-range communication design of the IAN may not support all nodes in an incident area. If a node is not able to connect to the IAN, he transmits his traffic via the jurisdictional area network. IAN devices must support a minimum range of 250 meters since this is the minimum required length of a fire hose.
- Jurisdiction Area Network (JAN): This is the main network for responders. It provides communications to remote areas from the incident location. JANs are made up of long-range communication nodes and multiple IANs. There may be multiple JANs within a region and they are assumed to span ranges of 5 to 110 kilometers.
- Extended Area Network (EAN): This network connects local, state and county jurisdictions. It is expected that the EAN will be connected via long-haul links such as wire or point to point microwave.

Networks are established depending on the size of the response to the incident. For small incidents requiring only local interdiction, an IAN may only be necessary. However, large-scale incidents may require the establishment of multiple JANs with out-of-area internet connectivity provided by an EAN. Figure 4.2 depicts the natural network hierarchy.

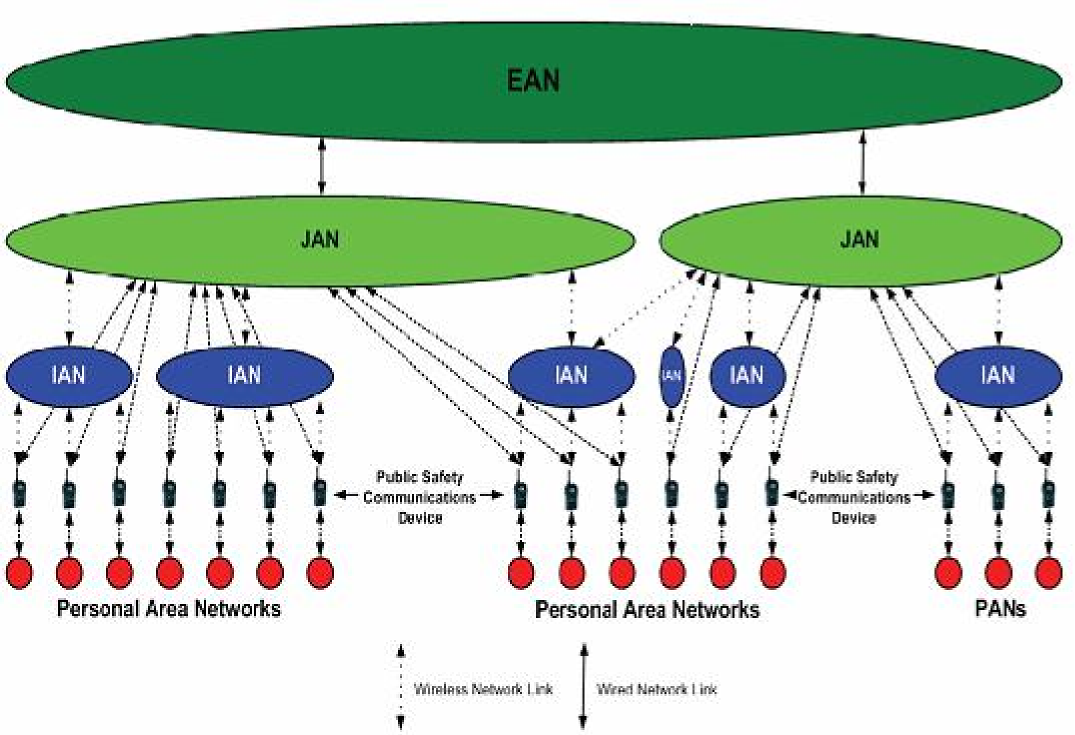


Figure 4.2: Network Hierarchy [28]

4.1.4 Network Voice Capabilities. Voice remains the most important mechanism for mission critical communications [62]. Therefore, it is a requirement for an effective public safety communications system. In order to send voice over a digital, wireless network, it must first undergo certain processes and interactions (Figure 4.3). These processes and interactions alter the voice transmission by injecting unwanted noise or delays. Any system, which supports public safety communications, is bound by certain standards concerning the transmission of voice.

4.1.4.1 Speech Encoding. Pre-processing is the first step that digital speech must undergo. In this step, the signal is detected, cleaned and enhanced. Coding involves the use of special algorithms, which

> seek to minimize the bit rate in the digital representation of a signal without an objectionable loss of signal quality in the process. High quality is attained at low bit rates by exploiting signal redundancy as well as the knowledge that

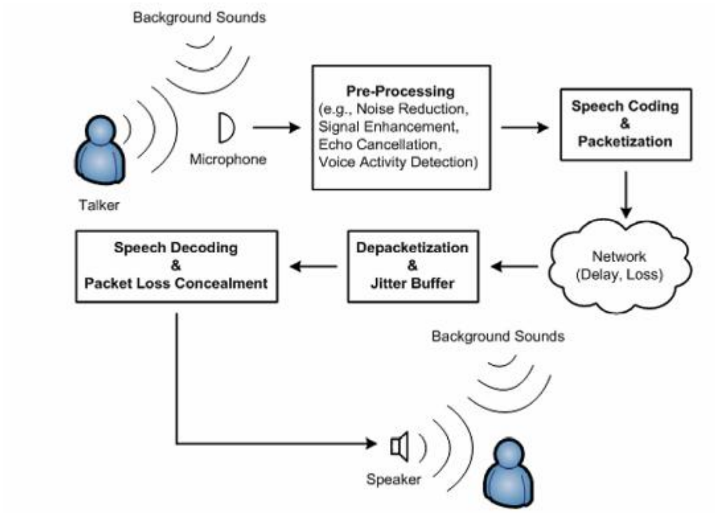
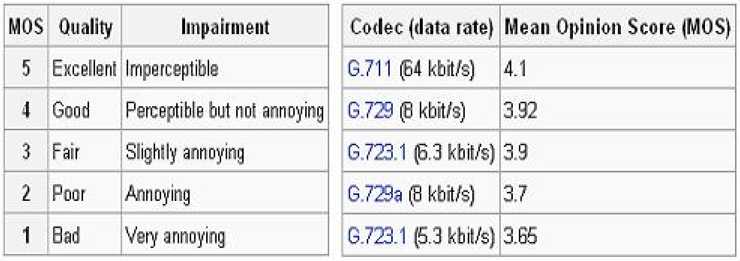


Figure 4.3: Digital Speech Encoding Process

certain types of coding distortion are imperceptible because they are masked by the signal [14].

Essentially, the coding process transforms high bit rate digital speech into a lower bit rate signal capable of more efficient transfer across the medium. The lower the bit rate, the lower the bandwidth required to transmit the signal. However, low bit rates normally translate to lower speech quality. There are various speech coding-decoding algorithms, or speech codecs, in use today and each one has differing levels of compression and sound quality. A standard system called the Mean Opinion Score (MOS) is used rate the level of quality of speech. Table 4.2 lists the most common speech codecs and their associated MOS. G.711 and G.729 codecs provide a level of sound quality sufficient for the public safety net and are recommended for use.

Table 4.2: Common voice codecs and their mean opinion score

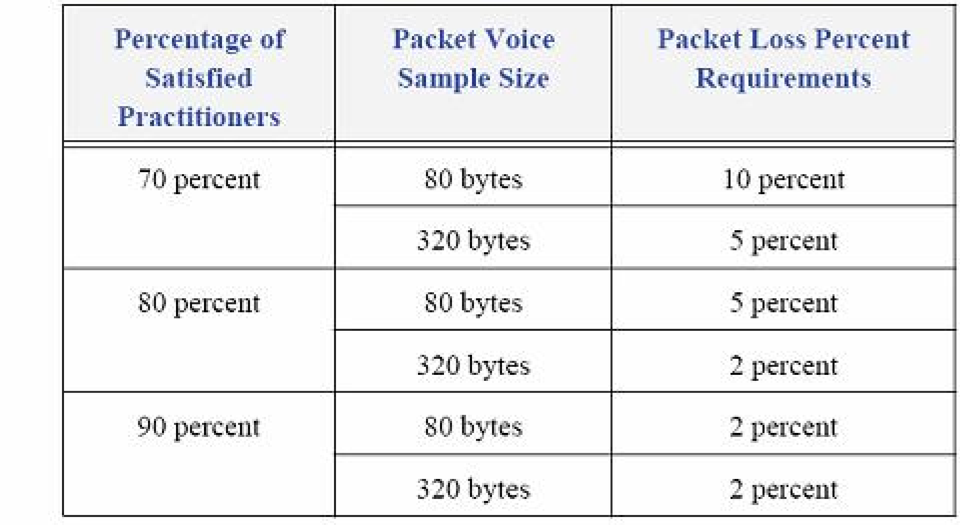


MOS	Quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

Codec (data rate)	Mean Opinion Score (MOS)
G.711 (64 kbit/s)	4.1
G.729 (8 kbit/s)	3.92
G.723.1 (6.3 kbit/s)	3.9
G.729a (8 kbit/s)	3.7
G.723.1 (5.3 kbit/s)	3.65

4.1.5 Network Packet Loss. Whenever information is sent across a network utilizing the Internet Protocol (IP), it is first segmented into smaller chunks or packets. This process is called packetization. Each packet consists of a header and the data to be transmitted. The header informs the network of the address of the device the packet is destined, the senders address, and the size of the data (in bytes). The entire process helps to prevent excessive delays in retransmitting data in the event it fails to reach its destination. Instead of a lengthy transmission waiting to finish before it can be retransmitted, small packets facilitate quick turnaround. From this process, it is evident that larger packets have different performance over the network than smaller packets. If large packets are dropped during speech transmission, it becomes more apparent to the listener than if small packets are dropped. However, smaller packets may require more system overhead as more packets are needed to transmit the same information. This can lead to greater transmission delays. Table 4.3 shows the results of a survey conducted by SAFECOM and contained in the SoR. For a rapidly deployable network for first responders, the minimum requirement for packet loss should be equivalent to the values needed for a seventy percent satisfaction rate.

Table 4.3: Packet Loss versus Satisfaction with Digital Voice [28]



Percentage of Satisfied Practitioners	Packet Voice Sample Size	Packet Loss Percent Requirements
70 percent	80 bytes	10 percent
	320 bytes	5 percent
80 percent	80 bytes	5 percent
	320 bytes	2 percent
90 percent	80 bytes	2 percent
	320 bytes	2 percent

4.1.6 End-to-End Delay. End-to-end delay refers to the time required for a transmission to be sent to the time it is heard. It is also referred to as mouth-to-ear delay.

End-to-end delays consist of various other delay components including: process delay, look-ahead delay, transmission delay, and propagation delay. Figure 4.4 shows a graph of the satisfaction level of customers as compared to the overall delay in the transmission. The solid line shows a non-packetized voice transmission (as with traditional telephone service) and the dotted line shows a packetized voice transmission using the G.711 codec [71]. The graph shows that mouth-to-ear delays of approximately 300 milliseconds equate to a seventy percent satisfaction rate for packetized data. However, the SoR states that for mission critical communications, the maximum mouth-to-ear delay should be no more than 150 milliseconds.

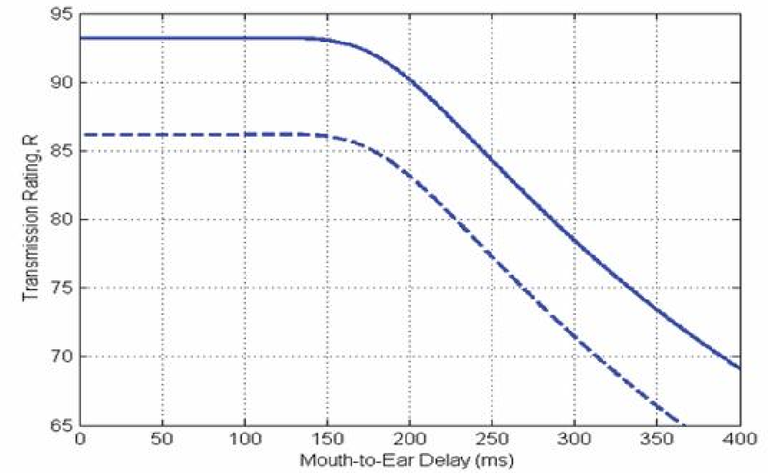
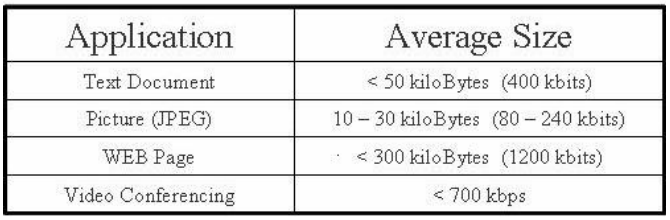


Figure 4.4: Mouth-to-Ear Delays for G.711 and G.107 Codecs [28]

4.1.7 Network Data Capabilities. Data consists of any non-voice related information transmitted across the network. It includes text, pictures, and video. The SoR states that both interactive, and non-interactive, data communications must be supported, and that data communications are becoming increasingly important to public safety personnel. Therefore, a network designed to support emergency responders must take into account the bandwidth demands of data users. Pictures and text require relatively small amounts of bandwidth. The average file sizes for common applications are shown in the table below. However, interactive, real-time video can put great demands on the network. Similar to digital voice, video undergoes compression algorithms before it is sent across the wireless network. There is a plethora of codecs available for video compression. The SoR states that a maximum delay of 150 milliseconds is desired for interactive video. The network should be implemented with a minimum of medium quality video, which can be accomplished using the H.264 codec.

Table 4.4: Common File Sizes



Application	Average Size
Text Document	< 50 kiloBytes (400 kbits)
Picture (JPEG)	10 – 30 kiloBytes (80 – 240 kbits)
WEB Page	< 300 kiloBytes (1200 kbits)
Video Conferencing	< 700 kbps

In addition to the performance requirements identified above, the SoR also provides many more requirements pertaining to public safety communications networks. However, they are mostly synonymous with the tasks identified in the NCOE JIC. Therefore, only the aforementioned requirements from this section are used in conjunction with the JIC tasks. The gap analysis section of this thesis contains the combined list and provides an overview of the proposed systems ability to complete each requirement.

4.2 Proposed Rapid Network Deployment System (RNDS)

The Rapid Network Deployment Systems (RNDS) concept of operation consists of utilizing 802.11 and 802.16 technologies to implement a hastily-formed communications network. The concept relies on pre-established systems that allow the Rapid Network Development Kit (RNDK) to enable the network through the establishment of a JAN node. In particular, the kit contains devices that other client nodes connect to. The following sections describe the proposed RNDS features and provide information concerning COTS equipment that can be used in support of the system. In general, users connect to short-range local area networks, which in turn connect to a jurisdictional area network. The JAN then connects to an internet PoP directly or through other JAN nodes.

4.2.1 Public Safety Communications Device (PSCD). PSCD are worn by public safety personnel and create a local personal area network around the user. Essentially, they are PDA type devices designed to military specifications for ruggedness. The devices use both 802.15 (Bluetooth) and 802.11 technologies. Bluetooth, with its range of 30 feet, is used to connect peripheral devices, such as GPS receivers and vital sign monitors to the primary PSCD. The PSCD acts as a master station for all of its client or slave devices. This allows freedom of movement for public safety personnel without a single, large and bulky unit to carry. PSCDs are not part of the RNDK; they connect to it via Incident Area Network (IAN) nodes. This connection is made through an 802.11a link operating at 4.9 gigahertz and providing 54 megabits per second of data rate. In the event a PSCD is not within the range of an IAN access node, it can automatically switch to an ad-hoc mode of operation and route its traffic through other PSCDs which have links to the access point. This ability allows for expansion of the local network beyond the direct range of the IAN access point.

In order to meet the SoRs minimum requirement of 250 meters of coverage over the 802.11a IAN, a wireless network adapter card with the appropriate transmit power and reception sensitivity is needed. An example is Ciscos CB20A adapter, which transmits at 54 megabits per second with a range of over 300 meters. This is accomplished with a transmit power setting of 13 dbm and the receiver sensitivity set at 1.58 watts [63], (where dbm is equal to a decibel referenced to 1 milliwatt). This card can be connected to the PSCD via the devices onboard slots.

Each PSCD is programmed with the users occupation type and unit information. This information, along with his GPS location data is routinely transmitted over the network. Each PSCD also contains an interactive display that allows the user to access Geographic Information Systems (GIS) maps of the area he is located. Overlaid on each map is the location of all other users on the network. The software application on the PSCD then can calculate relative distances the user is from others. Communications groups are also supported by the PSCD. Users can form talk groups, which include persons within certain proximities, persons located at a certain incident, or based on persons identification information. The application software, using information transmitted over the network, automatically determines the criteria and allows the selection for the user. The PSCD can also be used to contact any single person in the network by simply selecting the persons credentials from a stored library of users. The talk group features of the PSCD enhance individual usability and overall system collaboration as proposed in the knowledge management aspect of this thesis. Figure 4.5 shows a schematic of a PSCD.

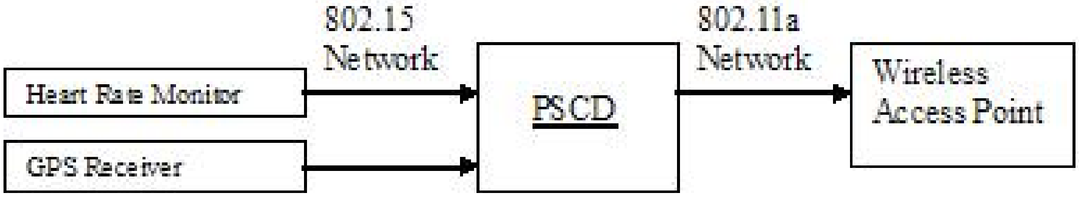


Figure 4.5: Schematic of the Public Safety Communications Device

Currently, the United States Army uses a device similar to the proposed PSCD. The Armys Commander Digital Assistant (CDA) is a small hand-held computer (Figure 4.6) which allows for voice communications, blue force tracking via GPS, and a host of other software enabled features that improve the situational awareness of the user.

Figure 4.6: U.S. Army Commander’s Digital Assistant

The CDA also can connect to both wireless networks and satellite networks. Expansion of the CDAs capabilities to include video and voice over IP technologies can be used to develop the proposed PSCD.

4.2.2 Incident Area Nodes. Incident area network (IAN) nodes are located on public safety vehicles such as police cars and fire trucks. They link responders within the incident area to one another and to remote locations, and connect to other incident sites which are in communications range. The host vehicle supplies power the IAN nodes.

IAN nodes consists of dual mode access points/routers, which support an 802.11a local network and provide an 802.16 (WiMAX) backhaul link to a jurisdictional area network (JAN) node contained in the rapid network deployment kit (RNDK). The proposed access point/router utilizes three separate channels to best support the traffic demands of the network (Figure 4.7). The communication equipment maker Proxim makes an access point with these features. The Proxim Meshmax 3500WM Tri-radio, WiMax subscriber and Wi-Fi Mesh access point uses one of its three channels to support 802.11a connections. This connection allows the PSCD to access the network. It uses its second 802.11 channel to automatically link itself to other Meshmax nodes within its range, and it uses the third channel to connect to the WiMax access (JAN) node for backhaul communications [61].

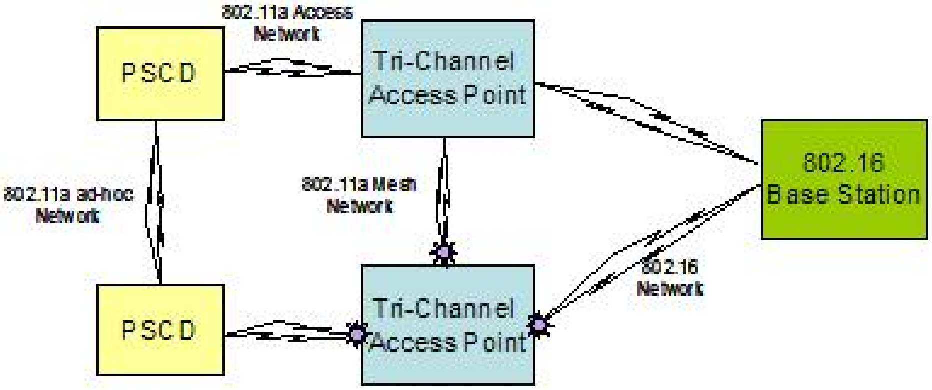


Figure 4.7: Three Channel Incident Area Network Schematic

The IAN nodes use of the three channels significantly increases network performance as nodes are not contending for the transmission medium and trying to send traffic over the same channel. Figure 4.8 highlights the significant performance difference of a single, dual, and three channel mesh network as the number of nodes increase. The graph shows that, unlike single and dual-channel mesh nodes, overall system capacity improves as the number of three-mesh nodes increase.

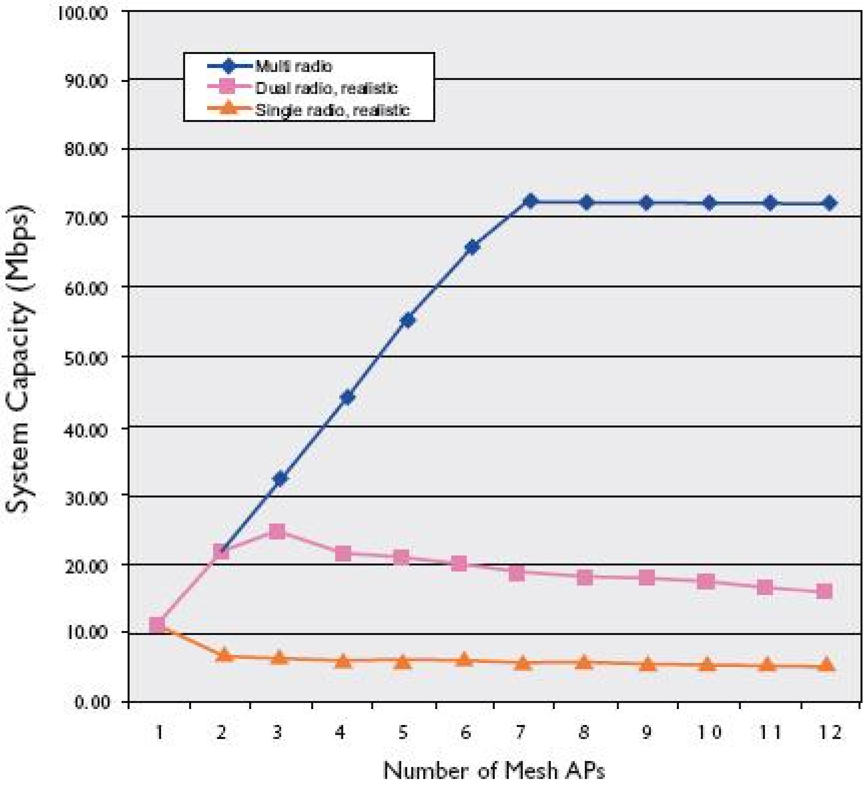


Figure 4.8: Performance comparison of single, dual, and triple channel mesh networks

This performance increase ultimately results in smaller delays across the network. In a single channel mesh configuration, packets which require more than three hops within the mesh can result in unacceptable voice delays across the network. In a three channel mesh configuration, 50 milliseconds or less delays can be maintained across as many as ten hops [53]. This is well within the required 180 millisecond or less delay for voice.

4.2.3 JAN Access Node. The primary enabler of the RNDS is the jurisdictional area network (JAN) access point. This node is contained in the Rapid Network Deployment Kit (RNDK) and is deployed to create a wireless network with an 802.16e (WiMax) backbone. The JAN access point contains a WiMax access point/ router connected to an omni-directional antenna. With this equipment, a wireless network can be created which extends to approximately 30 miles with an appropriately elevated antenna. This fits the SoRs definition of the size of a jurisdictional area network (JAN) of 5 to 110 kilometers. Any IAN node within range of the JAN access point through its WiMax channel as long as the SSID and the proper authentication code is entered into its device settings. The omni-directional mode of WiMax supports data rates of up to 70 megabits per second. The JAN node interconnects all IANs within range to an IP network. With a 30 mile radius coverage, a single JAN node could theoretically cover 2800 square miles. The city of New Orleans spans approximately 4200 square miles [58]. Therefore, two nodes could cover a city of its size. WiMax can also operate in a line-of-sight directional mode. The use of a directional antenna increases the range of the technology to over 100 miles. However, this thesis proposes the omni-directional mode of operation. This mode reduces both the need for multiple antennas in the RNDK the systems power requirements.

A mesh network of JAN nodes is proposed. Each node automatically connects itself with other WiMax nodes within its range. Links are made until one or more JAN nodes is within range of an Internet point of presence (PoP), at which point a connection can be made to deliver internet and Expanded Area Network (EAN) services to the system. It is anticipated that an operable Internet PoP will be available within the 30 mile coverage area of a single JAN node. If not, another JAN node could be erected at a location with an Internet PoP or to provide a hop link for the network to a more distant location. This proposal assumes an agreement concerning regional WiMax service usage is negotiated prior to an incident. Also, since WiMax uses a time division multiple access (TDMA) scheme for users to gain access to the transmission medium, the hop problem associated with 802.11 does not exist. Data can undergo many hops through the WiMax network with very little additional delay.

An example WiMax device which could be used for the JAN node could be Proxims Tsunami MP.11 series of base stations. In particular, the High Power 5054-R-LR version provides support for speeds up to 120 kilometers per hour and ranges up to 20 miles. It is designed to operate with standard 110/240 voltages and has a maximum power consumption of 20 watts. It also is designed with an integrated omni-directional antenna and is light-weight at less than 15 pounds. The base station and antenna are depicted in figure 4.9 below.

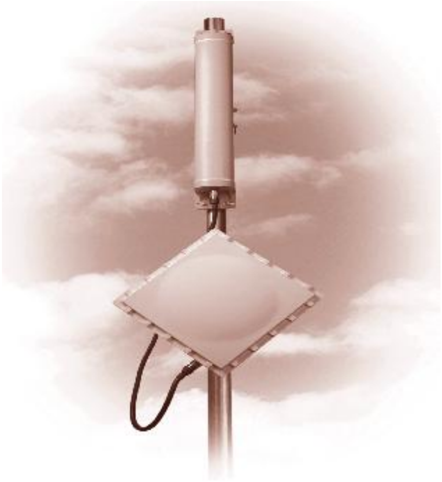
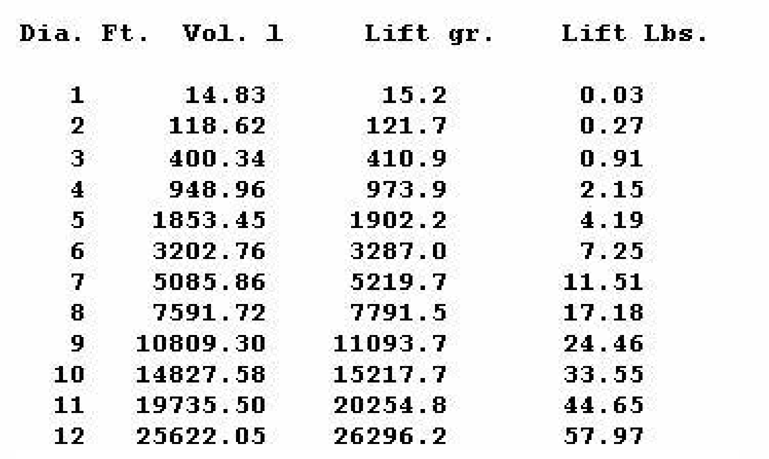


Figure 4.9: Proxim's Tsunami MP.11 high power WiMax base station [61]

4.2.4 Balloon Airlift Platform. One of the most important features of the RNDK is ability to lift a WiMax JAN node above the clutter of the normal operating environment. The kit utilizes a moored balloon to lift a network node to up to 300 feet. This altitude gives an unobstructed line-of-sight distance of 50 miles assuming the receiving node will be at ground level. The dimension of the balloon needed to lift the base station node device was then determined. WiMax Base station antenna equipment with an attached gyro-stabilizer weighs about 8 pounds. Rope and electrical cable weights vary, but typical braided one-half inch polypropylene rope weighs less than two pounds per one hundred feet and has tensile strengths greater than two hundred pounds [44]. Therefore, the estimated weight of the ropes was less than 5 pounds.

In order to provide power to the node, a wire cable must extend from the generator to the access point. A typical one hundred foot length of 12-gauge electrical cords weighs less about 7 pounds. Therefore, an estimated 21 pounds of weight was added for the electrical cable. The total lift needed is 37 pounds. Next, the size of the balloon needed to lift the node is determined. Table 4.5 shows a listing of balloon sizes versus their lift capacity and the amount of helium needed to fill them. According to the table, a balloon of approximately 11 feet diameter is needed. Typical commercial helium cylinder capable of providing 6,500 liters of helium weighs approximately 125 pounds and is 51 inches high and nine inches in diameter [64]. Therefore, four of these bottles are needed as part of the kit.

Table 4.5: Balloon Size vs Lift Capacity



Dia. Ft.	Vol. l	Lift gr.	Lift Lbs.
1	14.83	15.2	0.03
2	118.62	121.7	0.27
3	400.34	410.9	0.91
4	948.96	973.9	2.15
5	1853.45	1902.2	4.19
6	3202.76	3287.0	7.25
7	5085.86	5219.7	11.51
8	7591.72	7791.5	17.18
9	10809.30	11093.7	24.46
10	14827.58	15217.7	33.55
11	19735.50	20254.8	44.65
12	25622.05	26296.2	57.97

The U.S. Army uses a tethered balloon system called the Rapidly Elevated Aerostat Platform (REAP) as shown in figure 4.10. It is designed to be deployed in five minutes and can stay aloft for 10 days [55]. It also has a payload capacity of 35 pounds (not including tether) and can be transported on the back of a standard size truck.

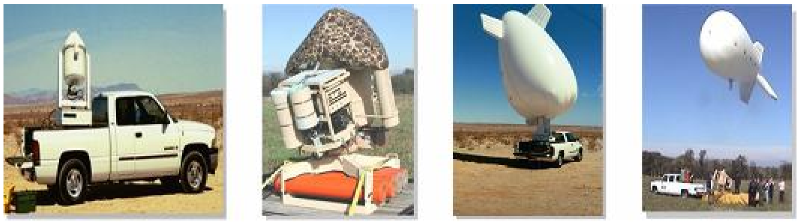


Figure 4.10: REAP Deployment [10]

4.2.5 Power Generation for Network Access Point. In order to generate power for the WiMax access point, an electric generator is needed as part of the kit. As mentioned previously, the intent of the RNDK is to provide a temporary, compatible network until more long-term solutions are established. Since wide ranges of electric generators are available with varying performance feature. The Honda EB5000 is recommended for it portability and its up to 12 hour operating time. The generator provides both 110 and 240 volts power at a maximum of 5000 watts. Furthermore, the generator weighs only 214 pounds and can easily be transported on a truck.

4.2.5.1 Summary of RNDS Nodes. The basic overview of the RNDS devices was presented. However, assumptions are made concerning network management functions, such as bridge devices, and optimization software. These aspects are beyond the scope of this thesis in that they are not a part of the RNDK so they do not detract from the goal of espablishing an expeditious network. Bridge devices are either at remote locations, or, if needed, built into the JAN router and can be left at ground level. Network management software is normally designed to support remote configurations over the wireless network, so it can be housed at any location. Voice over IP (VoIP) call management equipment is also needed in the system to support voice communications, and gateways are required to connect to the public switched telephone network (PTSN). However, these devices are commonly used to provide VoIP services and are therefore assumed as understood and not further described. Also, the equipment can be remotely located and does not constitute additional RNDK equipment.

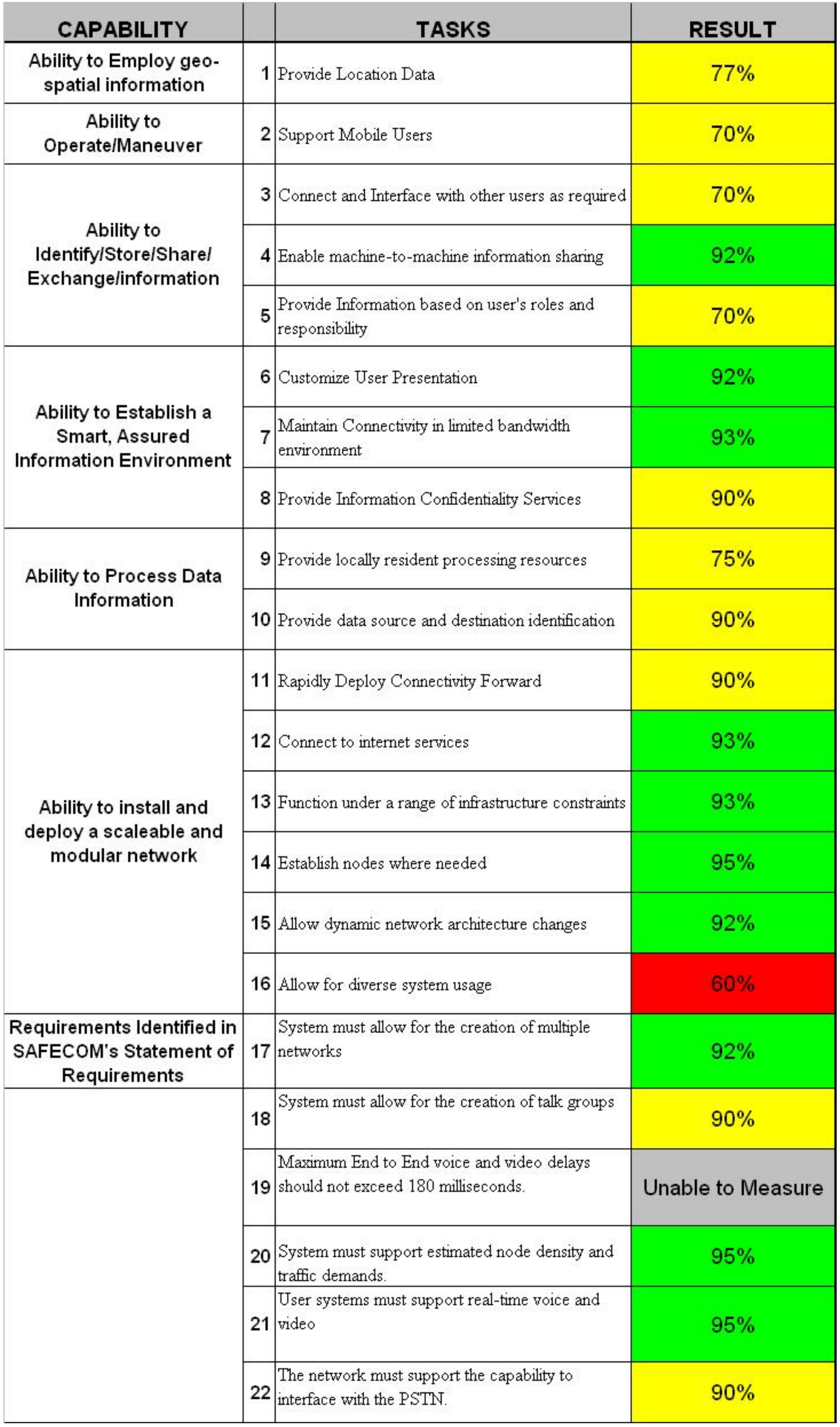
There are also various types of protocols which must be in use by devices on the networks. These protocols, such as the Real Time Protocol (RTP) allow real-time voice, video and other services to be accessed. Both 802.11 and 802.16 support the use of these protocols so any limitations to their usage reside in the user devices used to access the network. It is assumed that the protocols needed to communicate over the network will be resident in the user devices as required.

4.2.6 Comparing Tasks to Proposed Networks Features. The earlier identified tasks required for a public safety communication system to support an incident management environment are compared to the features proposed for the RNDS. This was done to determine where gaps exist in the system. A subjective rating is assessed on the RNDSs ability to perform each task. In Table 4.6 below, each tasks is shown with an assigned percentage value and color code. The percentage value represents the overall accessed ability of the proposed system to perform the task. The color codes correspond to the percentage values, where a grade of 90 to 100 percent is green and means the system performs the task very well, 70 to 90 percent is yellow and means the system performs the task adequately, and less than 70 percent is red and means the system performs the tasks poorly. Appendix C contains further justification of the grades assigned to each task.

Analysis of each task revealed that the proposed solution adequately fulfills the tasks and requirements for a rapidly deployable network for first responders. The only tasks which were not accessed as 70 percent or greater were the ability for the system to allow diverse usage and the ability of the system to limit maximum end-to-end delays to less than 180 milliseconds.

The proposed RNDS design consists primarily of 802.11 and 802.16 wireless networks. As described in chapter two of this thesis, public safety personnel use a wide array of devices and various technologies to communicate. The RNDS only allows for compatible wireless devices to access the network. Therefore, it cannot accommodate traditional radio systems unless gateway equipment is used to interconnect the two

Table 4.6: System tasks and RNDS effectiveness



CAPABILITY		TASKS	RESULT
Ability to Employ geo-spatial information	1	Provide Location Data	77%
Ability to Operate/Maneuver	2	Support Mobile Users	70%
Ability to Identify/Store/Share/ Exchange/information	3	Connect and Interface with other users as required	70%
	4	Enable machine-to-machine information sharing	92%
	5	Provide Information based on user's roles and responsibility	70%
Ability to Establish a Smart, Assured Information Environment	6	Customize User Presentation	92%
	7	Maintain Connectivity in limited bandwidth environment	93%
	8	Provide Information Confidentiality Services	90%
Ability to Process Data Information	9	Provide locally resident processing resources	75%
	10	Provide data source and destination identification	90%
Ability to install and deploy a scaleable and modular network	11	Rapidly Deploy Connectivity Forward	90%
	12	Connect to internet services	93%
	13	Function under a range of infrastructure constraints	93%
	14	Establish nodes where needed	95%
	15	Allow dynamic network architecture changes	92%
	16	Allow for diverse system usage	60%
Requirements Identified in SAFECOM's Statement of Requirements	17	System must allow for the creation of multiple networks	92%
	18	System must allow for the creation of talk groups	90%
	19	Maximum End to End voice and video delays should not exceed 180 milliseconds.	Unable to Measure
	20	System must support estimated node density and traffic demands.	95%
	21	User systems must support real-time voice and video	95%
	22	The network must support the capability to interface with the PSTN.	90%

technologies. However, the RNDS concept uses what the authors believe is the technology most likely to be accessible to all responders in the wake of a disaster, namely IP based computers and radio devices.

4.3 Knowledge Management Results

The proposed physical solution is designed to provide ubiquitous communications where anyone can communicate with anyone else. The point is made throughout this thesis and in the network-centric literature, though, that actually operating in this fashion may cause more problems than it solves: information overload can occur, and command and control structure can become ineffective. Referring again to the GAO report cited in Chapter Two of this thesis, ubiquitous communications does not equate to effective communications. The results of the mathematical and computational analysis that explore the knowledge management aspect of this problem are now discussed.

4.3.1 Graph Theory Results. Graph theory is used to describe an optimal topology of response node, or *response topology*, in the disaster response context. The response topology is analogous to the "edge" of an organization as described in the network centric literature. The metric *collaboration capacity* describes the ability of the system to meet the collaboration needs of the nodes in the system. A topology-independent *maximum collaboration capacity* is calculated, then the three subject topologies are compared with this optimum solution. The results of this analysis also point to other useful metrics used in the simulation study.

4.3.1.1 Topology-independent solution. In order to maximize the load on the system and thereby analyze the system's maximum capacity to accommodate the load, each network node must be able to share its full measure of collaboration. Since a star substrate is assumed, each response node, r_i, is connected to $C2$, and the edge weighted at one or $l(C^2)/n$, whichever is less. The expression for excess load of each response node, if any, is therefore

$$l_e(r_i) = l(r_i) - (l(C^2)/n) \tag{4.1}$$

where $l(r_i) = 1$ and $n > 5$.

The system collaboration capacity, $CC(R)$, is the sum of the edge weights. It is calculated independently of response node topology by assuming the load is distributed evenly throughout a homogeneous system, R, where $R = G - C2$. The assumption of homogeneity leads to the following:

1. R is a k-regular graph; $d(r_i) = k$
2. Edges in R are weighted equally; $w_j = w_{j+1}$

Since the system collaboration capacity is equal to the sum of the edge weights and each edge has the same weight,

$$CC(R) = \sum_{j=1}^{e(R)} w_j = e(R) \cdot w_j \tag{4.2}$$

where e(R) is the number of edges in R, or the *size* of R.

Since R is k-regular, the degree sum formula for a k-regular graph,

$$e = \frac{1}{2}kn \tag{4.3}$$

is used to provide an expression for $e(R)$ in terms of k and n.

Applying Eq. 4.3 to Eq. 4.2:

$$CC(R) = \frac{1}{2}knw_j \tag{4.4}$$

In general, a node's load is distributed evenly among its incident edges, and the weight of each edge is

$$w_j = \frac{l(v)}{d(v)} \tag{4.5}$$

The load of each response node in R is given by Equation 4.1 and its degree is k. Therefore,

$$w_j = \frac{1}{k}(1 - \frac{l(C^2)}{n}) \tag{4.6}$$

Applying Equation 4.4, the collaboration capacity of R is therefore

$$CC(R) = \frac{1}{2}n(1 - \frac{l(C^2)}{n}) \tag{4.7}$$

Finally, the collaboration capacity of the entire system, G is

$$CC(G) = \begin{cases} n & n \leq l(C^2) \\ l(C^2) + \frac{1}{2}n(1 - \frac{l(C^2)}{n}) & n > l(C^2) \end{cases} \tag{4.8}$$

Figure 4.11 shows the relationship between $CC(G)$ and the number of nodes in the system. As Equation 4.8 implies, $CC(G)$ increases directly with n until $n = l(C^2)$. This represents a normal operations situation where the $C2$ node is not overloaded, and collaborates directly with its subordinates. As the $C2$ node becomes overloaded, however, response nodes must collaborate with each other in order to share their full measure of collaboration. As indicated in Equation 4.8 and shown in Figure 4.11, the system collaboration capacity increases at a rate of one half n. It can be shown that this relationship is maximal, and is the standard against which the subject topologies are now measured.

4.3.1.2 Hierarchical topology. The NIMS prescribes adding additional layers of hierarchy as a method for accommodating additional response nodes. The NIMS does not, however, specify where additional command and control nodes come from or what their capabilities are. This model assumes that that any node added below $C2$ is a

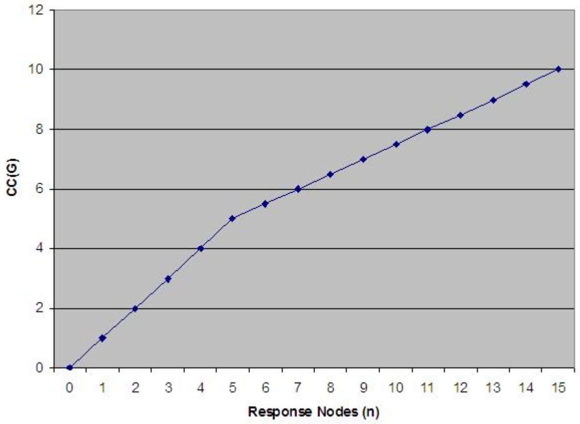


Figure 4.11: Maximum Collaboration Capacity increases with Number of Nodes

response node with unit load. In other words, response nodes are subordinate to other response nodes (Figure 4.12. Mathematically, the first five response nodes are in the first *neighborhood* of $C2$; additional response nodes are in higher order neighborhoods.

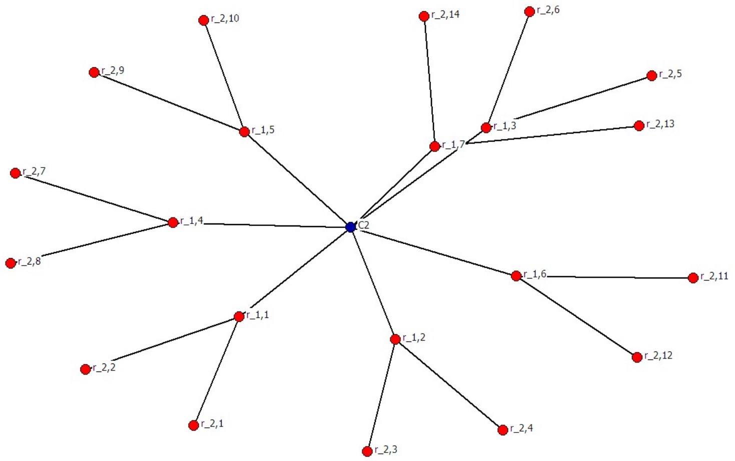


Figure 4.12: Hierarchical Topology

The neighborhood, $\Gamma(v)$, of a vertex v is the set of vertices adjacent to v, but not including v itself. $\Gamma^2(v)$ represents the second neighborhood of v where some or all vertices in $\Gamma(v)$ have their own neighborhoods. More generally, $\Gamma^a(v)$ is the a^{th} neighborhood of v. In this model the i^{th} response nodes in the first neighborhood of $C2$ is written $r_{1,i}$; the i^{th} response node in the second neighborhood of $C2$ is $r_{2,i}$.

Beginning with the star graph where $n = l(C^2)$, a response node is added. Since $l(C^2)$ is maximal, an edge is added between the new node, $r_{2,i}$ and an existing response node, $r_{1,i}$. If, as the model assumes, the $C2$ node is afforded its full measure of collaboration, then $w_{C^2,r_{1,i}} = 1$. Since nodes cannot be overloaded $w_{r_{1,i},r_{2,i}}$ must be zero. If, however, it is assumed that $r_{1,i}$ collaborates evenly with both $C2$ and $r_{2,i}$, $w_j = \frac{1}{d(r_i)}$,

$$w_{C^2,r_{1,i}} = \frac{1}{2} \quad and \quad w_{r_{1,i},r_{2,i}} = \frac{1}{2}$$

Assuming only one additional C^2 layer, it can be shown that the collaboration capacity of a hierarchical topology is:

$$CC(h) = l(C^2) + \sum_{i=1}^{n} CC(r_{a,i}) - 1 \tag{4.9}$$

$$\text{where } n \leq l(C^2)$$

If the load of all nodes in the first neighborhood remain at one, the collaboration capacity of the system remains constant and equivalent to $l(C^2)$. Generally, this formula indicates that additional $C2$ nodes must be added to the system to increase collaboration capacity.

4.3.1.3 Complete topology. Figure 4.13 shows a complete subgraph of $\Gamma(C^2)$ where each node is connected to every other node. Since a complete graph is k-regular such that $k = n - 1$, the collaboration capacity calculation for this graph is identical to that described in the topology-independent case above. In other words, the collaboration capacity of a complete subgraph topology is maximal, and therefore meets this requirement for an optimal topology. The complete subgraph topology demonstrates however, that while necessary, this characteristic is not sufficient of an optimal topology.

Since $w_j = \frac{1}{d(r_i)}$, and in the complete topology $d(r_i)$ is maximal, w_j is minimal. In this network, w_j represents the amount of collaboration between two nodes. Minimum edge weight, therefore, is an undesireable characteristic. Hanneman and Riddle explain

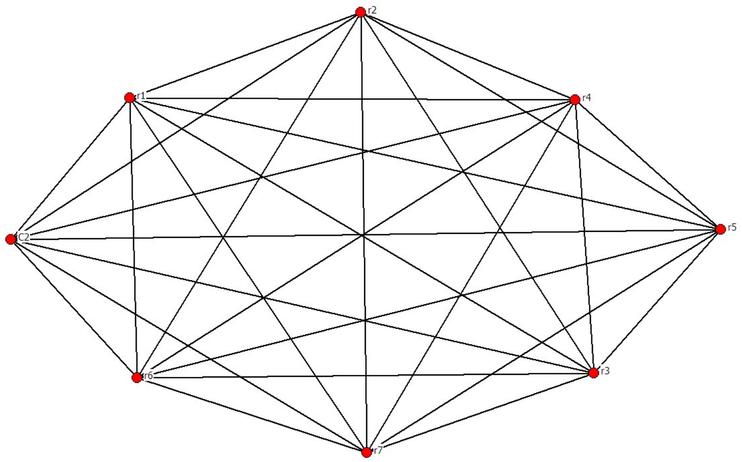


Figure 4.13: Complete graph topology

that social network theorists set thresholds on edge weights below which, for practical purposes, an association does not exist. [36] This finding is also in agreement with Miller's channel capacity discussed in Chapter Three of this thesis.

A macro-level way of describing this constraint is network density, which is the ratio of edges in a network that do exist to those that could exist. High density corresponds to low edge weight in this model, which is undesireable. Since all the edges that can exist in a complete graph do, its density is maximal at one. High density is also undesireable in small world networks discussed in Chapter Two of this thesis. In the small world context, high density implies the breakdown of communities of interest because of global interactions in a spatial graph.

4.3.1.4 Hybrid topology. Figure 4.14 shows a topology that meets the maximum collaboration capacity requirement while observing the constraint of low density:

This topology is constructed as follows:

1. The algorithm begins by connecting all response nodes (r_i) to the central node ($C2$).
2. When n is greater than $l(C^2)$, edges are added between response nodes to form *components*. These edges represent peer-to-peer collaborations between and among

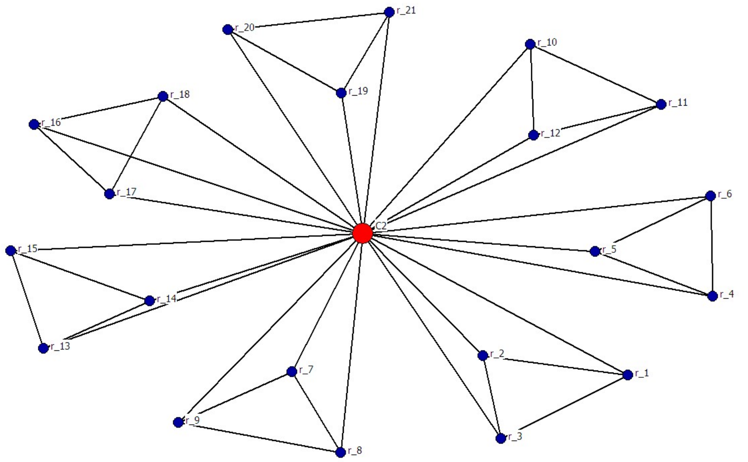


Figure 4.14: Proposed topology

response nodes. When modeled computationally, components are formed based on node attributes (e.g. geographical proximity). *Note the term component is used differently here than in graph theory literature.* In this model components are created as follows:

(a) The next node above $l(C^2)$ is connected to both $C2$ and one of the empty nodes such that there are $l(C^2) - 1$ independent members of R and one component with two nodes. This is done iteratively until $n = 2 * l(C^2)$.

(b) As additional nodes are added they join the smallest component so that no component is more than one node larger than any other. When n is an integer multiple of $l(C^2)$, every component has an equal number of nodes.

(c) Edges are weighted as described above.

This topology is integrated with a complete command and control system as described in Chapter Three. The system is then evaluated using both social networking metrics described below and the measure of effectiveness, weighted in-degree.

4.3.2 Simulation Results.

4.3.2.1 Network Characteristics. Due to the limitations of UCINet, the model used to obtain the following network results does not exactly match the mathematical model described above. Specifically, the results described below were obtained using a symmetric, unweighted graph. While UCINet is capable of analyzing asymmetric, weighted data, the weights must be in integer form; the weights used in this research are in decimal form. An attempt is made, however, to recover from this by creating a simulation model analogous to the symmetric one used in UCINet. While the edges in this second simulation model are weighed, no preference is given to the relationship between a response node and its $C2$ node. This research "accident" actually turns out to be quite fortuitous in that a system that gives preference to the command and control system (the mathematical model) is now compared to an "ad-hoc" network where no such preference is afforded. These two systems are referred to as *integrated* and *ad-hoc*, respectively. Despite this misqueue, a great deal of qualitative information is gained in the graph theory results.

Each data point in the figures below is the average of three simulation iterations. Given the qualitative nature of these results and the lack of outliers, three iterations is considered sufficient by the authors.

4.3.2.2 Density. Figure 4.15 shows that graph density, or the ratio of the edges that exist to the number of possible edges, remains low for all workloads (number of nodes) until the range increases above five.

The reason for this is obvious when two networks are compared side by side. In Figure 4.16 where $R = 5$, response nodes can only reach halfway across a jurisdiction. There is some cross-jurisdictional collaboration between response nodes, but the jurisdictional neighborhoods are still fairly well defined. They are not apparent at all, however, in Figure 4.17 where $R = 10$.

Above a range of five, therefore, the networks become dense; an undesirable characteristic for reasons already discussed.

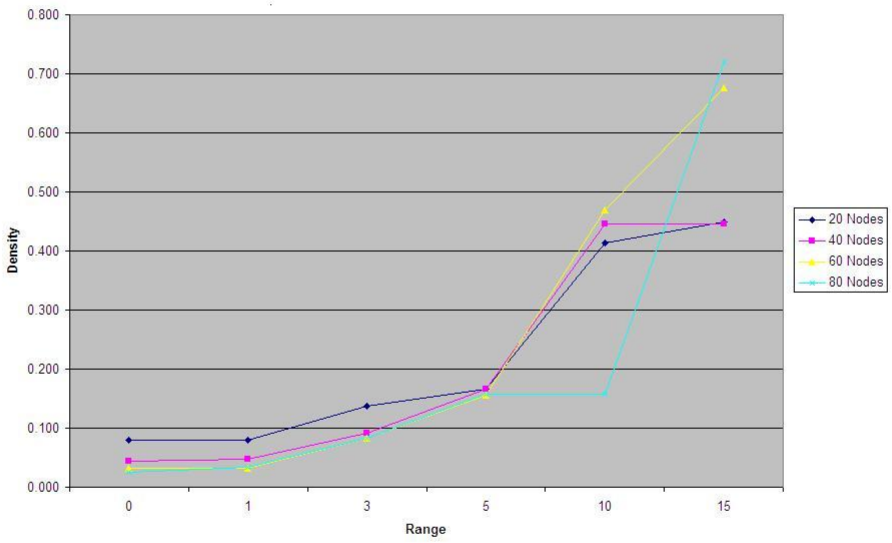


Figure 4.15: Density vs Range

4.3.2.3 Clustering Coefficient. Hanneman advises that in "assessing the degree of clustering, it is usually wise to compare the cluster coefficient to the overall density." [36] By viewing Figure 4.18 in light of Figure 4.15 one can see why. Between $R = 0$ and 5, density is low while the clustering coefficient exhibits interesting behavior. Above $R = 5$, both clustering coefficient and density increase linearly. Combining the two pieces of information shows that above $R = 5$ the local and global characteristics of the network become indistinguishable, just as Watts says they will in a spatial graph. In other words, the network becomes one big cluster instead of a set of smaller ones.

What of the clustering coefficient's behavior between $R = 0$ and 5? Clustering is initially low at $R = 0$ and $R = 1$, increases dramatically between $R = 1$ and $R = 3$, then increases linearly. This behavior is expected. While response nodes are initially connected to their assigned $C2$ node, there are no connections between or among response nodes. Clustering is therefore low. At $R = 3$ response nodes in a jurisdiction are highly clustered among themselves, but there are few external connections. As range increases so do the number of external connections; clustering becomes linear as response nodes connect on a

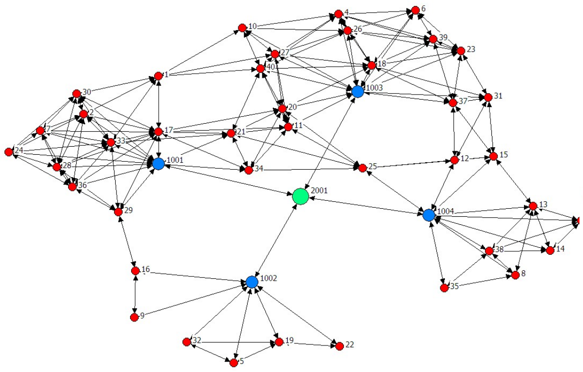


Figure 4.16: n = 40; R = 5

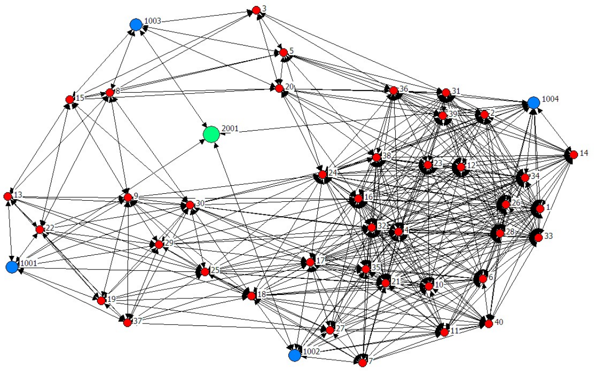


Figure 4.17: n = 40; R = 10

global scale, and the network becomes one big cluster. The reader is referred to Appendix # for a visual example of each network iteration.

4.3.2.4 Centrality. As first responders collaborate among themselves to perform their tasks, it is reasonable to assume that the influence or control that their assigned command and control node has over them decreases. Social network theorists use the metric *centrality* to measure the degree of influence any node has over others. If node A is on a path connecting nodes B and C, A is in a position to influence B and C assuming there is not an edge between them. A is therefore *between* B and C. A node's *betweenness centrality* is the number of such paths that node is on. The betweenness centrality of all nodes in a network can be aggregated into the *network centrality index* (NCI) used here. NCI is the "degree of inequality or variance in our network as a percentage of that of a perfect star network of the same size." [36] In a star network, the central node is maximally central, the others have zero centrality. Variance or inequality in a star network with respect to centrality is a maximum, so the star topology is used as a normalizing construct in betweenness centrality. NCI is particulary pertinent in this research since the "as-is" system, the hierarchical topology, is a star. The amount of variance from the hierarchical topology described by the NIMS is therefore measurable.

The results of the betweenness centrality analysis is shown in Figure 4.19, which lead the authors to no quantitative conclusions regarding betweenness centrality. As

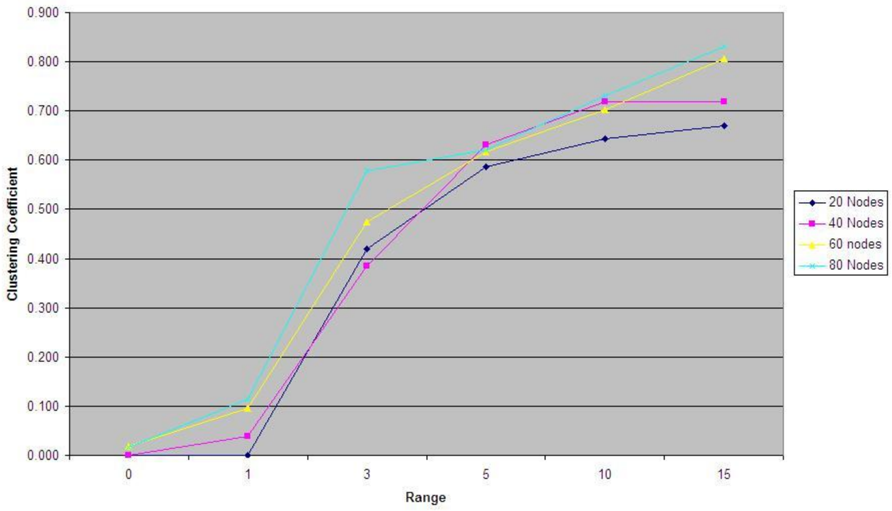


Figure 4.18: Clustering Coefficient vs Range

anticipated, the centrality, which is considered analagous to influence or control, decreases when subordinate nodes collaborate. Unlike density and clustering coefficient, however, there is no knee in the centrality curve. Work domain analysis is required to set a minimum threshold on betweenness centrality to which these results may point. Since, for example, low density and high clustering coefficient occur at a range of three, perhaps a useful threshold for betweenness centrality is 50 percent. Further researh is needed in this area, but this metric proves qualitatively useful later in this thesis.

4.3.2.5 Distance. The hypothesis regarding the distance metric is that as nodes are added and/or range values are increased, the average geodesic distance in the graph drops significantly. This hypothesis springs from Watts' work on small worlds. As Figure 4.20 shows, however, distance is not significantly affected by either workload or range.

This result codifies the nature of small world networks, the difference between relational and spatial graphs, and the role of the command and control system in this model. In Watts' model, all nodes are the same, and they are either connected or they are

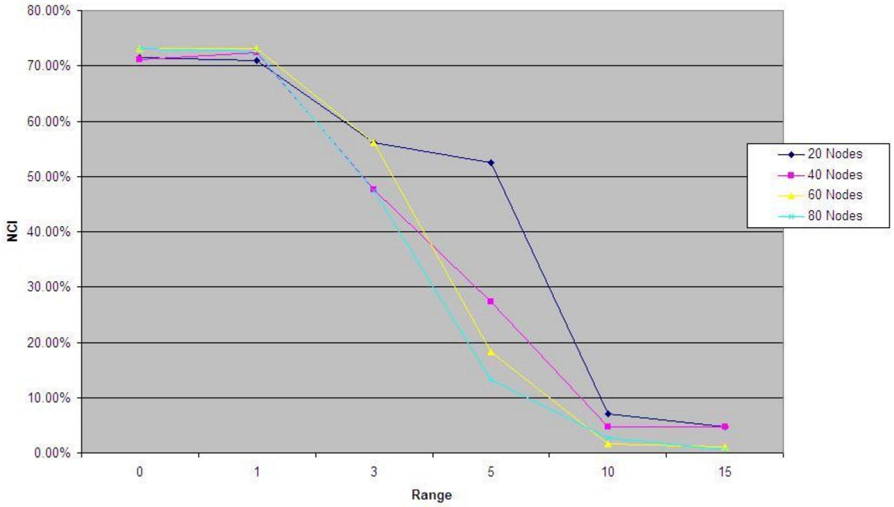


Figure 4.19: Betweenness versus Range

not. His spatial graph model is the equivalent of an ad-hoc network. He shows that spatial graphs cannot display small world characteristics because local edges become global as the distance metric is increased. In this model, the command and control system globally connects the response nodes, so the distance is pre-compressed. There is no need to add global edges; they already exist. One would not expect, therefore that the average distance between any two nodes would decrease significantly until the distance metric is increased sufficiently to create global edges. In other words, since the distance across the network is pre-compressed, no further compression takes place until the network is sufficiently dense to nullify the effect of the command and control system. This is, in fact what is seen when Figure 4.20 is compared with Figure 4.15. Average distance drops significantly when range exceeds five, which is the same point where density increases.

4.3.2.6 Network Characteristics Summary. Although the model used to generate network analysis metrics does not exactly match the integrated model, viewed together they illuminate desireable qualities of a disaster response network. Specifically low density combined with high clustering are telling characteristics of what is thought

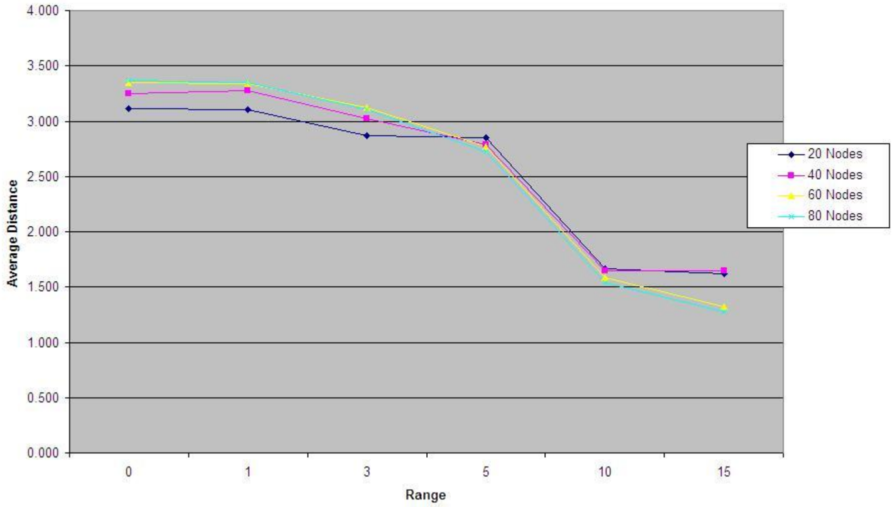


Figure 4.20: Distance versus Range

to be a desireable network. Centrality of the command and control nodes is also a key characteristic, and seems to be inversely related to the clustering. Finally, although distance is commonly touted as a key network metric, it is shown here to be a function of network density in a spatial graph. What remains is the "so what" factor. The next section answers this question by proposing a measure of network effectiveness that compliments and validates the graph theory metrics.

4.3.3 Node Effectiveness Results. Network effectiveness is measured using the *average weighted in-degree*, $D^{+}_{avg}(r_i)$, metric described in Chapter Three. It is the average of the *total weighted in-degree*, $d^{+}_{tot}(r_i)$, of each response node in the network. A response node's total weighted in-degree represents the amount of collaboration it receives from its neighbors. Ideally, $d^{+}_{tot}(r_i)$ is one, meaning the amount of collaboration a response node receive is neither too much (greater than one) or too little (less than one). The weighted in-degree for a network of response nodes is found by taking the average of all $d^{+}_{tot}(r_i)$.

4.3.3.1 Hypothesis One. Hypothesis One states: When span of control is not exceeded, collaborations degrade effectiveness.

Figure 4.21 shows the effect of range on the average weighted in-degree, $D^{+}_{avg}(r_i)$, for 20 response nodes (command and control nodes are not considered). This graph shows that as range increases above one and collaborations begin to exist (see Section A.1), $D^{+}_{avg}(r_i)$ increases above one, and the response nodes are overloaded. Qualitatively it shows that when a network is not overloaded, collaborations degrade effectiveness. Figure 4.19 (20-node case) shows that the network metrics behave as expected: collaboration degrades effectiveness of the command and control system. When the system is not overloaded, this degradation is not necessary.

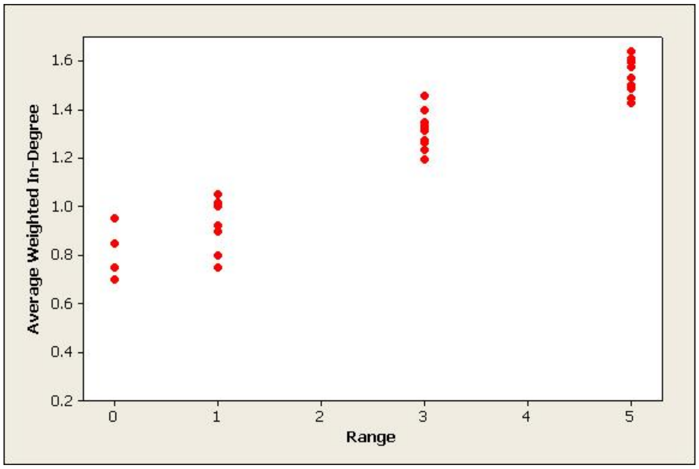


Figure 4.21: $D^{+}_{avg}(r_i)$ vs R, $n = 20$

4.3.3.2 Hypothesis Two. Hypothesis Two states: When span of control is exceeded, collaborations improve effectiveness.

This hypothesis is explained by examining the interaction between the number of response nodes and their range. The network metrics generated in UCINet indicate that the variation in system response is dominated by range. Using $D^{+}_{avg}(r_i)$ as the response and both the number of response nodes and range as independent variables, a two-way ANOVA study is conducted using the statistical analysis tool Minitab to evaluate system sensitivity to these two factors. Table 4.7, a standard ANOVA table shows the results of this ANOVA. The first column lists all the sources of variance in the model: number of nodes, N; range, R; the interaction of both N and R; and random error. The third column, labeled SS, shows the sum of the squared errors, which is the key indicator of the source of the variance. The results of the ANOVA clearly show that changes in the average in-degree are due overwhelmingly to changes in range.

Table 4.7: Two-Way Anova: Response vs N, R

Source	DF	SS	MS	F	P
N	2	0.3775	0.18877	192.58	0.000
R	3	12.5919	4.19731	4282.03	0.000
Interaction	6	0.0447	0.00745	7.60	0.000
Error	108	0.1059	0.00098		
Total	119	13.1201			

S = 0.03131 R-Sq = 99.19

Figures 4.22 and 4.23 demonstrate this point even more clearly. The scatter-plot of average in-degree to changes in number of nodes shows very little variation in system response. The scatterplot of average in-degree versus range, however shows a clear system response, namely, average in-degree increases as range increases.

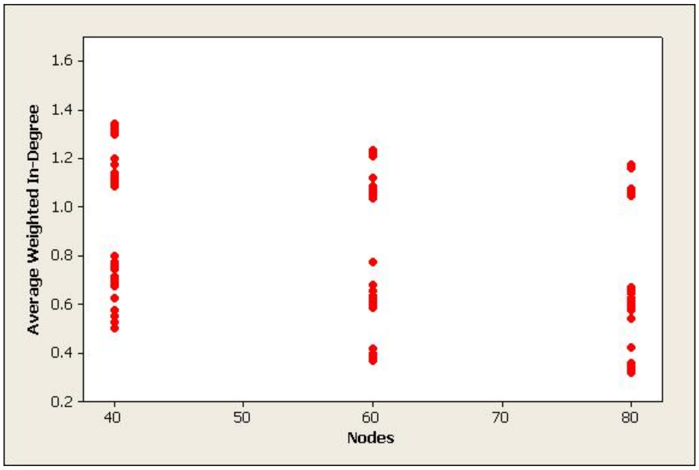


Figure 4.22: $D^{+}_{avg}(r_i)$ vs n

Figure 4.23 also shows that $D^{+}_{avg}(r_i)$ is close to optimal with a mean of 1.08 at $R = 3$, but increases to an overload condition with a mean of 1.24 at $R = 5$. This indicates that there is an optimal range at which response nodes collaborate to maximize system effectiveness. Comparing this data with the results of the network study, one can see that optimal effectiveness coincides with desirable network characteristics. Notably the greatest increase in clustering occurs at $R = 3$ while density remains low.

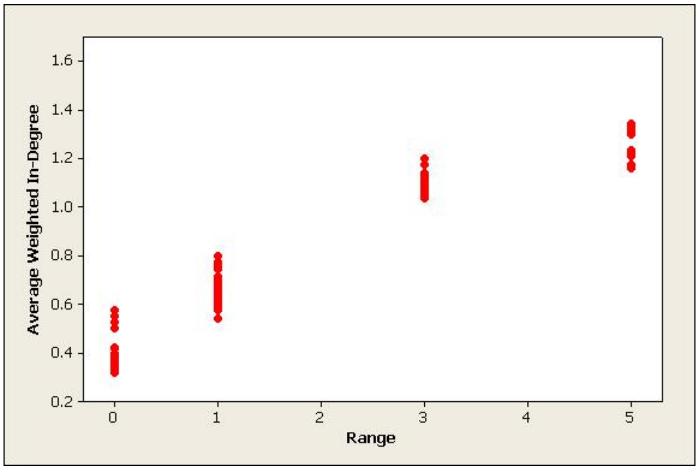


Figure 4.23: $D^{+}_{avg}(r_i)$ vs R

4.3.3.3 Hypothesis Three. Given the results of the two-way ANOVA, the ad-hoc and integrated networks are compared at each range, zero through five. These results are shown in Figures 4.23 and 4.24, respectively. Where $D^{+}_{avg}(r_i)$ for the ad-hoc network becomes overloaded above a range of three, it becomes asymptotic at one in the integrated network. Moreover, there is a great deal of variability in system response in the former case whereas variation decreases in the latter. This may indicate that the integrated network is more robust to variation in system attributes. These data show, for example, that an ad-hoc network performs most effectively when range is three whereas the integrated network performs well at ranges between zero and five.

While network analysis is not performed on the integrated system, the finding that increasing the distance metric beyond a certain limit results in undesirable behavior is

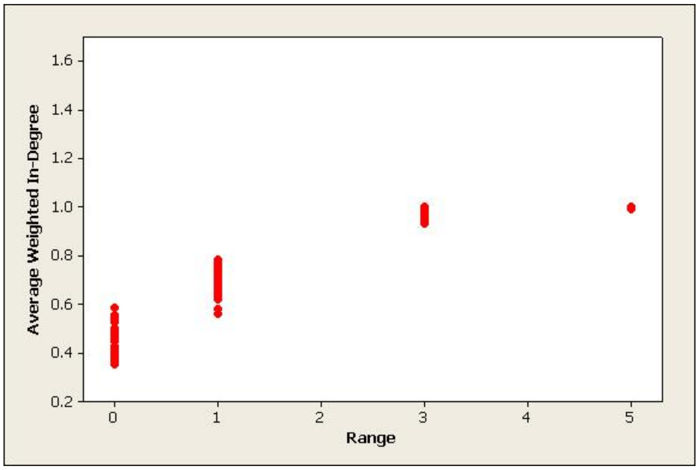


Figure 4.24: $D^{+}_{avg}(r_i)$ vs R in an Integrated Network

considered applicable. Specifically, distance values beyond the local to global transition point, i.e. where density blows up, are undesirable. Using this theory, range values beyond five are considered untenable even in an integrated system.

4.3.4 Knowledge Management Summary. This analysis shows how effective communication, or in this case, effective collaboration, can be realized given ubiquitous communication technologies. Graph theory provides an optimized "edge" topology which is integrated into a hierarchical command and control system as proposed by network-centric theorists. Computational modeling and simulation shows how network characteristics and performance vary as *distance* varies. Distance in this model is geographical, but could be any attribute that defines a spatial graph as defined by Watts. Network density and clustering coefficient are found to be key network characteristic metrics in the combined collaborative-hierarchical network defined in this research; together they show where the network transitions from local to global. Weighted in-degree appears to be a valid measure of response node effectiveness, and when extended to the entire graph by averaging $d^{+}_{tot}(r_i)$ over all response nodes, it becomes a measure of network effectiveness. Together the network characteristic and network effectiveness results indicate that collaboration among "edge" entities generally improve the effectiveness of an overloaded network. Moreover, a collaborative "edge" environment properly integrated with a fixed command and control system has advantages, hoped for by small world theorists, over a purely ad-hoc network.

4.4 Summary

The results of the physical solution analysis indicate that a system for providing ubiquitous communications in a disaster response scenario is achievable with current technologies. The results of the knowledge management study show that entities within a disaster response environment can be organized to create the effects envisioned in the Tenets of Net-Centric Warfare.

Response nodes in this model represent incident commanders, which, in an operational environment, would have a three-channel IAN node on their vehicle. The three-channel technology enables the ad-hoc meshing with other IAN nodes, which increases network bandwidth as IAN nodes are added within range of one another. This increasing bandwith accommodates the increasing collaboration capacity seen in the mathematical model as nodes are added and begin to collaborate with one another. Another IAN channel using 802.16 WiMax technology is used to link incident commanders with emergency operations centers, which may have either a resident JAN node or an IAN node that connects via a JAN node. The simulation model uses a 20 mile by 20 mile area representing a county jursdiction. A JAN node would provide wireless connectivity at this jurisdictional level allowing the municipal-level EOCs to utilize IAN systems and connect to their subordinates via the county-level JAN node.

The authors' vision is that this combined technical/organizational proposal is a first step on an iterative process of disaster response system improvement. Chapter Five describes what are thought to be the next steps in this process.

V. Conclusion and Recommendations

5.1 Conclusion

This research investigates hastily-formed collaborative networks using the National Incident Managment System and Hurricane Katrina as context. Two aspects of this problem are identified: providing a rapidly-deployable ubiquitous communications network and managing the human aspects of that network so that individuals within it are neither overloaded nor underserved. The first aspect requires a physical solution, the second a knowledge management solution. A Rapid Network Deployment System (RNDS) is proposed to facilitate interoperable emergency response communications in the wake of a major incident, and a methodology is proposed to organize network entities into communities of interest that allow them to collaborate effectively.

The goal of providing ubiquitous communications in an austere environment such as the post-Katrina Gulf Coast region is achievable using current technology and equipment. Specifically, the 802 family of wireless technologies provides the mobility, range, and bandwidth needed, as well as the ability to efficiently scale to support large, Katrina-sized disaster response. Current 802.11 technologies allow individual personnel to create and integrate into an incident area network (IAN). The enabling device is a three-channel wireless router. One of the three channels uses 802.11 to connect responders in an incident area. A second 802.11 channel allows IANs to interact with each other creating a MESH network in an ad-hoc fashion. Instead of overloading the network, available bandwidth actually increases as IAN nodes are added. The last channel uses 802.16 to connect with a jurisdicional area network (JAN), which, in-turn, connects the emergency response network to an internet point of presence (POP).

Because it imposes the threat of information overload on its users, ubiquitous communications is a necessary but not sufficient condition for an effective disaster response network. Information within the system must be managed so the right information gets to the right place at the right time. This is referred to as knowledge management. Using network-centric operations as a theoretical starting point, a mathematical model of an optimal "edge" network topology, dubbed a hybrid topology, is proposed. When integrated with a hierarchical command and control system, the combined disaster response network displays desireable network characteristics and effectiveness.

5.2 Recommendations for Further Research

The technical and knowledge management solutions proposed in this thesis are complimentary, and can be viewed as a first step toward an operational solution to the problem of creating hastily-formed collaborative networks. The next steps toward realizing a deployable network are work domain analysis, information system development, and discrete event simulation.

The attribute used to define collaborations in the simulation model is *range*. If two response nodes are within a certain range of each other in this model, an edge is created between them, and they collaborate. It is unlikely that, in the real world, first responders want to collaborate with one another solely on the basis of their geographical proximity. They might collaborate, for example, because they are the same type (police, fire, rescue, etc.). No attempt is made in this research to define the attributes which might cause two first responders to collaborate with one another or quantify the strength of a relationship. Work domain analyisis is needed to define a set of attributes that facilitate collaboration, quantify the strength of a collaboration, and set a threshold on strength below which a collaboration effectively does not exist. Furthermore, information systems must be developed that identify, assign, and track network entities and their relationships in an operating environment, and that then calculate measures of network effectiveness such as those proposed in this thesis.

Once work domain analysis is conducted, a realistic network can be modeled and simulated. By "equiping" the nodes in this new model with technologies such as those proposed in the physical solution section of this thesis, a discrete event simulation study can be conducted using a tool such as OpNet. Evidence from this research can then be used to further specify the social network, develop other technical solutions, or propose future avenues of research and experimentation.

5.3 Contributions to the Body of Knowledge

The work done in this thesis to propose a physical solution to the problem of providing ubiquitous communications in a disaster response scenario validates the top-down, capabilities-based approach embodied in the JCIDS process. Using the DoD's JCIDS approach and DoD and DHS documentation, the authors identify a feasible solution to this important problem using technology that is currently available and in use.

In the knowledge management realm, the authors used the idea of viewing organizations as networks to analytically show the value of collaboration and to numerically demonstrate the utility of the small world concept. The value of collaboration is shown by applying it to a hierarchical "edge" topology and measuring the *collaboration capacity* of the resulting network. A theoretical maximum collaboration capacity is derived, and then used as a metric for evaluating the utility of an experimental topology. The hybrid topology, which captures the concept of communities of interest, is shown to be optimal using the maximum collaboration capacity criterion, and a constraint that the network have low density. The hybrid topology is then integrated into a hierarchical command and control to form a complete network model. The social network metrics (density and clustering coefficient) are shown to be key indicators of network behavior. Specifically high clustering combined with low density are characteristics of a "good" network. These metrics show that a real world (spatial) network can have desireable small world behavior. Finally, the advantages of an integrated network, which has a strong command and control system, over an ad-hoc network are shown using the metric *weighted in-degree*, a measure of effectiveness derived herein.

Appendix A. Sample Responders Networks

This appendix contains the graphs of the networks described throughout this research. They allow the reader to visualize the various topologies and associate metrics with a physical system.

A.1 20 Response Nodes

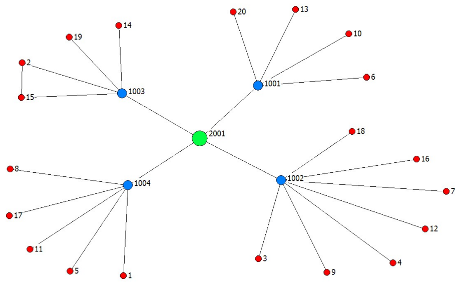


Figure A.1: nodes = 20; range = 0

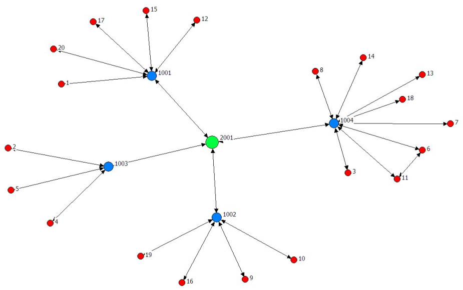


Figure A.2: nodes = 20; range = 1

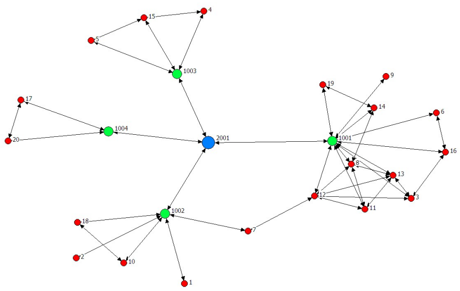


Figure A.3: nodes = 20; range = 3

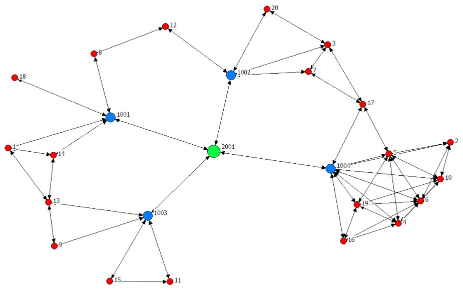


Figure A.4: nodes = 20; range = 5

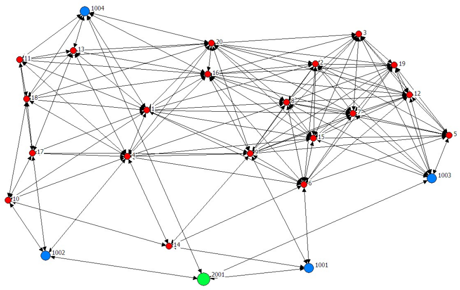


Figure A.5: nodes = 20; range = 10

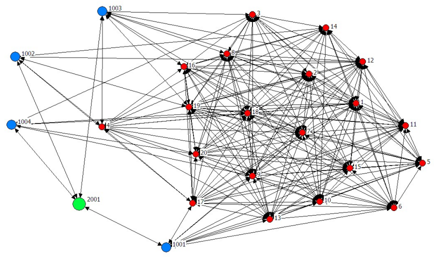


Figure A.6: nodes = 20; range = 15

A.2 40 Response Nodes

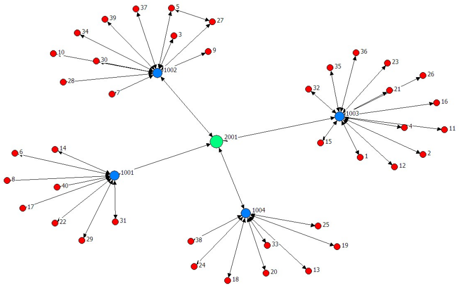


Figure A.7: nodes = 40; range = 0

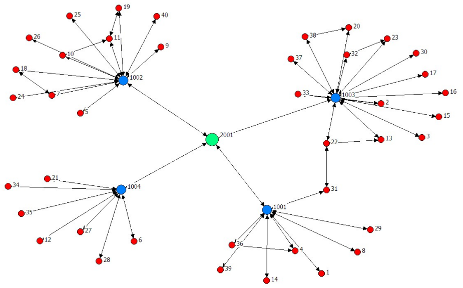


Figure A.8: nodes = 40; range = 1

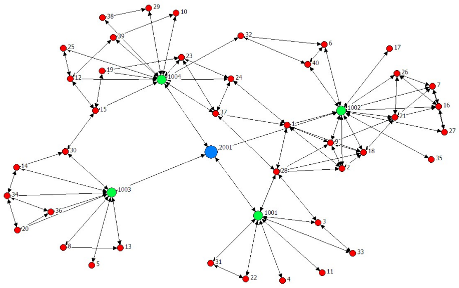


Figure A.9: nodes = 40; range = 3

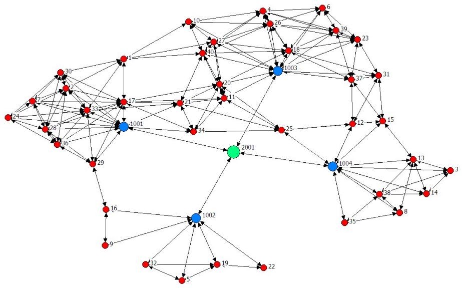


Figure A.10: nodes = 40; range = 5

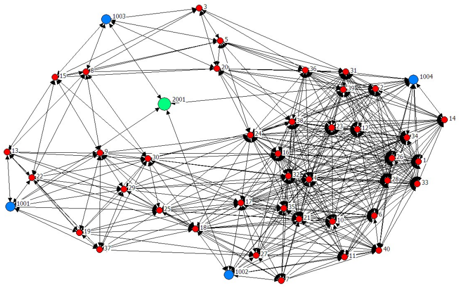


Figure A.11: nodes = 40; range = 10

A.3 60 Response Nodes

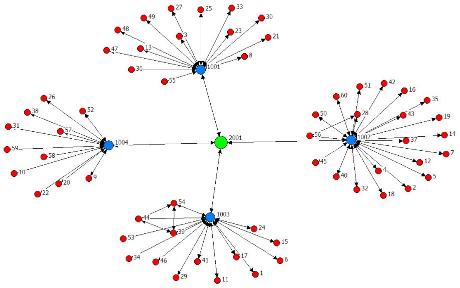


Figure A.12: nodes = 60; range = 0

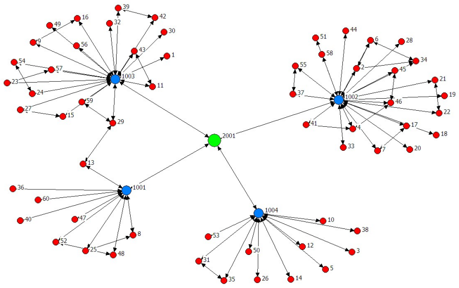


Figure A.13: nodes = 60; range = 1

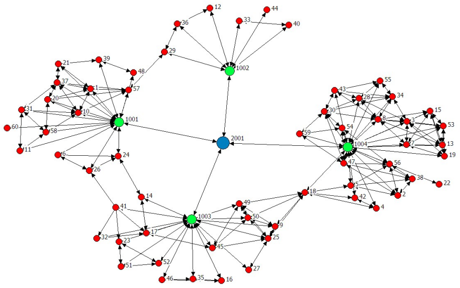


Figure A.14: nodes = 60; range = 3

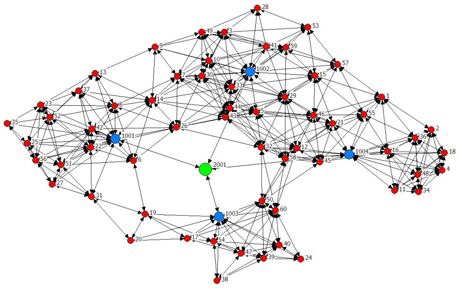


Figure A.15: nodes = 60; range = 5

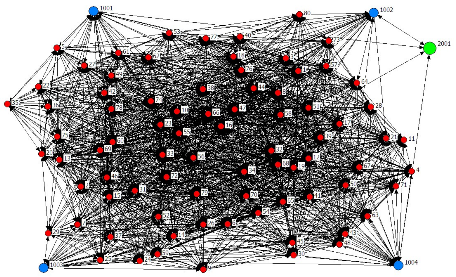


Figure A.16: nodes = 60; range = 10

A.4 80 Response Nodes

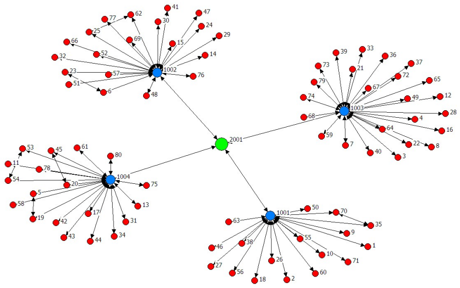


Figure A.17: nodes = 80; range = 0

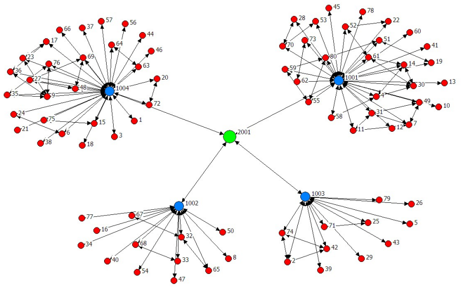


Figure A.18: nodes = 80; range = 1

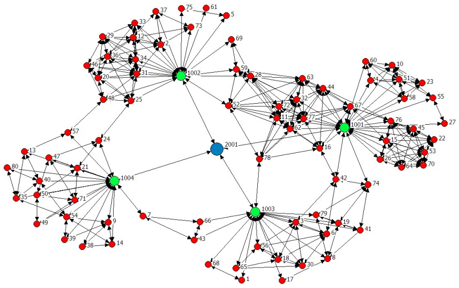


Figure A.19: nodes = 80; range = 3

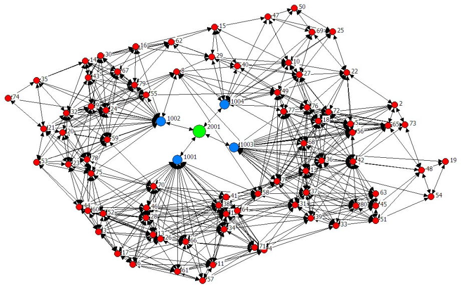


Figure A.20: nodes = 80; range = 5

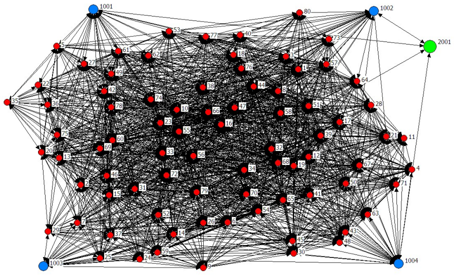


Figure A.21: nodes = 80; range = 10

Appendix B. Simulation Documentation

The final version of the simulation used to generate the disaster response network is AttribGen_4.0.xls. The simulation executes in Microsoft Excel 2003 sp2.

B.1 Overview

The simulation is based on a 2 mile by 2 mile disaster area. The area is divided into four 1 square mile jurisdictions, each with a jurisdiction commander. Incidents are generated and assigned random locations within the disaster area. One responder is assigned to each incident and inherits the incidents location. The responders commander is based on the jurisdiction in which the incident is located.

B.2 Parameters Worksheet

This sheet serves as the basis for the disaster area. Inputs include the number of responders that will be assigned to incidents within the disaster area. The number of different (incompatible) communication systems. The range that will be used to establish connections between responders for the purpose of collaboration.

B.3 IncidentAtt Worksheet

This sheet generates incidents equal to the number of responders that will be placed in the disaster area. The incidents are assigne an identification number and random X and Y coordinants that correspond to tenths of miles from the northeast most corner of the disaster area. The incident is also assigned a responsible commander depending on the jurisdiction in which the incident is located. C^2 nodes have responsibility for incidents according to the following:

- C^2 node 1001 (0,0) to (9,9)
- C^2 node 1002 (10,0) to (19,9)

- C^2 node 1003 (0,10) to (9,19)
- C^2 node 1004 (10,10) to (19,19)

B.4 Responders Worksheet

This worksheet generates the responders. Each responder has an ID number, type code, type, assignment, X and Y coordinate, Responsible C^2, and equipment type.

B.4.1 Type. Responders are assigned a random type from the set of {Fire, Police, Rescue, Medical}.

B.4.2 type code. The type code corresponds to the the type of responder accoding to the following:

- 1 = Police
- 2 = Fire
- 3 = Rescue
- 4 = Medical

B.4.3 Assignment. Responders are given an assignment number which corresponds to the ID number of an incident from the IncidentAtt Worksheet. Each responder is assigned to one incident

B.4.4 XLoc. This is the X coordinate of the incident to which the responder is assigned.

B.4.5 YLoc. This is the Y coordinate of the incident to which the responder is assigned.

B.4.6 Resp C2. This is the jurisdiction commander to whom the responder reports. This value is inherited from incident to which the responder is assigned.

B.4.7 Equip Type. This number represents the type of communication equipment the responder has. The equipment type is randomly generated based on the number of incompatible communication systems specified in the Parameters Worksheet.

B.5 CC_Adj Worksheet

This is an adjacency matrix describing the hierarchical relationship between responders and the command and control node to which they report. A one at the intersection of row x and column y indicates no collaboration exists between vertex x and vertex y. A zero at the intersection indicates the absence of collaboration.

B.6 Seperation_Dist Worksheet

This is a square matrix describing the physical distance in tenths of miles between row X and column Y for responder nodes. Distance between responders and command and control is always represented as a zero to prevent physical distance from preventing communication between a responder and his jurisdictional commander.

B.7 Seperation_Adj

This square matrix describes adjacency between responders by comparing their physical seperation as described in the Seperation_Dist Worksheet to the maximum range allowed for a connection based on proximity. The maximum allowable range for a proximity connection is input on the Parameters Worksheet.

B.8 Comm_Adj

This square matrix described adjacency between responders based on compatibility of communication equipment type. Responders with matching communication equipment are considered adjacent.

B.9 SepComm

This matrix determines the adjacency of responders based on the combination of separation adjacency and communcation equipment adjacency.

B.10 SepComm_inDeg

This matrix assigns a weight to each edge between adjacent responders. The edge weights are determined without preference for command and control.

B.11 SepCom_inDegV2

This matrix assigns a weight to each edge between adjacent responders. The edge weights are determined with preference given to command and control.

Appendix C. Evaluation of Rapid Netword Deployable System Against Required Tasks

1. - Capability: Ability to employ geo-spatial information
   - Task: Provide Location Data
   - Grade: Adequate
   - Justification: Location data is provided to a users PSCD by GPS satellites. These satellites are line-of-sight. Whenever a user cannot acquire a satellite, his PSCD cannot transmit an accurate position. However, it is believed that in most cases, the users will be in satellite reception range.
2. - Capability: Ability to operate and maneuver
   - Task: Support Mobile Users
   - Grade: Adequate
   - Justification: 802.16 does not allow for unlimited speed. The technology is designed for speeds up to 120 kilometers per hour. The SoR implies that reasonable speeds are those which a helicopters and civil aircraft may fly. These speeds exceed the 120 kilometer per hour limit. Therefore, users in these vehicles would have limited communications.
3. - Capability: Ability to identify/store/share/exchange/data information
   - Task: Connect and interface with others as needed.
   - Grade: Adequate
   - Justification: Provided the user is in the network coverage area, he should have no problem connecting. However, precipitation may adversely affect the WiMAX signals, particularly if the system is implemented with frequencies above 10 gigahertz.
4. - Capability: Ability to identify/store/share/exchange/data information

- Task: Enable machine-to-machine information sharing
- Grade: Very Well
- Justification: Design characteristic of most wireless access devices.

5. - Capability: Ability to identify/store/share/exchange/data information
   - Task: Provide Information based on users role
   - Grade: Very Well
   - Justification: Periodically, the PSCD sends out user identification information over the network. Therefore, customized data can be presented to each user. However, individuals not access the network with a PSCD may not support for this service.
6. - Capability: Ability to establish a smart, assured, information environment
   - Task: Customize user presentation
   - Grade: Very Well
   - Justification: User presentations are modifiable on the PSCD. This is an application activity and can be enabled by software.
7. - Capability: Ability to establish a smart, assured, information environment
   - Task: Maintain connectivity in limited bandwidth environment
   - Grade: Very Well
   - Justification: PSCDs are capable of transmitting both voice and data over the IP network. When bandwidth is limited such that high bandwidth information cannot be transmitted, the small sized identification packets can still be sent. The design of security protocols such as WEP and WPA (which are normally utilized on the network) are authenticated to the network with low bandwidth information contained in each packets header. As long as these packets are received, the user should stay connected to a limited bandwidth connection.
8. - Capability: Ability to establish a smart, assured, information environment

- Task: Provide information confidentiality services
- Grade: Very Well
- Justification: Each access node uses WEP encryption to prevent ease dropping on information passed over the network. Other applications, such as the advanced encryption standard (AES) algorithm are commonly used on devices to encrypt information and allow only the intended recipient to decipher the data.

9.
- Capability: Ability to establish a smart, assured, information environment
- Task: Provide locally resident processing resources
- Grade: Adequate
- Justification: The proposed PSCD design and most other wireless access devices have this ability. However, all devices connecting to the network may not.

10.
- Capability: Ability to process information.
- Task: Provide data source and destination information
- Grade: Very Well
- Justification: This information is contained in each IP packet sent over the network.

11.
- Capability: Ability to install and deploy a scaleable and modular network
- Task: Rapidly deploy connectivity
- Grade: Very Well
- Justification: The primary enabler of the RNDS is the WiMAX JAN node. This node can be deployed very quickly if a pre-configured kit, as described in chapter four of this thesis, is used. Also, the system is scalable by design of the IAN and JAN nodes. IAN nodes use multiple frequencies to control traffic. Other IAN nodes within range were automatically configured into the network.

Further, as more nodes entered the network, overall bandwidth available to each node increases. JAN nodes also feature auto detection capabilities, which allowed then to automatically connect with other nodes.

12.
- Capability: Ability to install and deploy a scaleable and modular network
- Task: Connect to Internet Services
- Grade: Very Well
- Justification: If a single WiMAX access point cannot reach an internet point of presence, it must hop to other nodes until it finds one. In certain cases, there may not be an internet point of presence within range of the available WiMAX nodes, and therefore, internet connectivity may not be available. However, these cases are believed to be rare.

13.
- Capability: Ability to install and deploy a scaleable and modular network
- Task: Function under a range of infrastructure constraints
- Grade: Very Well
- Justification: The proposed design of the system enables it to operate independent of the existing infrastructure.

14.
- Capability: Ability to install and deploy a scaleable and modular network
- Task: Establish nodes where needed.
- Grade: Very Well
- Justification: The system is designed so standard sized trucks can carry each network node. Furthermore, the kit could be lifted by helicopter to its desired location.

15.
- Capability: Ability to install and deploy a scaleable and modular network
- Task: Allow dynamic network architecture changes.
- Grade: Very Well

- Justification: The two underlying wireless technologies, 802.11 and 802.16 allow for mobility and rapid hand-offs of users from one access point to another. Also, the proposed mesh configurations of the network all for efficient system scaling.

16.
- Capability: Ability to install and deploy a scaleable and modular network
- Task: Allow diverse system usage
- Grade: Poor
- Justification: The proposed RNDS design consists primarily of 802.11 and 802.16 wireless networks. As described in chapter two of this thesis, public safety personnel use a wide array of devices and various technologies to communicate. The RNDS only allows for compatible wireless devices to access the network. Therefore, it cannot accommodate traditional radio systems unless gateway equipment is used to interconnect the two technologies.

17.
- Capability: Ability to support SAFECOMs requirements
- Task: Allow for the creation of multiple networks
- Grade: Very Well
- Justification: IAN and JAN networks are established and connected to EANs. Bridge devices, which separate networks into domains, are assumed as auxiliary equipment and not described in the overall systems description. Their functionality is assumed sufficient.

18.
- Capability: Ability to support SAFECOMs requirements
- Task: Allow for the creation of talk groups
- Grade: Adequately
- Justification: The proposed PSCD and the DHS proposed P25 IP radios can support talk groups. However, the ability of other wireless devices to support

talk groups would be dependant on the applications resident on the machine. Also, it is required and assumed that voice-over-IP (VoIP) call management equipment is resident in the network to support call group features.

19.
- Capability: Ability to support SAFECOMs requirements
- Task: Maximum end-to-end voice and video delays do not exceed 180 milliseconds.
- Grade: Unable to Measure
- Justification: This requires further testing of the networks performance characteristics under load and the ability to measure performance over all of the networks. However, the high bandwidth links on the network and the low data rate codecs in use would likely support delays less than 180 milliseconds, provided traffic loads are not excessive.

20.
- Capability: Ability to support SAFECOMs requirements
- Task: Support estimated network node density and traffic demands
- Grade: Very Well
- Justification: The number of persons in a JAN is estimated to be 30. Typical single WiMAX base stations can support up to 1500 users at moderate traffic loads. Only in situations were a large number of responders are operating in a small area with limited IAN nodes would traffic density likely become a problem.

21.
- Capability: Ability to support SAFECOMs requirements
- Task: The Network should connect to the public switched telephone network (PTSN)
- Grade: Adequate
- Justification: It is required and assumed that voice-over-IP (VoIP) call management equipment and gateways are resident in the network to support standard calling features, such as connection to the PTSN network.

22.

- Capability: Ability to support SAFECOMs requirements
- Task: The system should support both real-time voice and video
- Grade: Very Well
- Justification: The network topology and equipment used at all levels of the network allows for both voice and video traffic to be transmitted in real-time. It is assumed that the required protocols to support the services are present in the network.

Bibliography

1. Alberts, David S. and Richard E. Hayes. *Power to the Edge*. DoD Command and Control Research Program, 2003.

2. Alberts, David S. and Richard E. Hayes. *Code of Best Practice: Campaigns of Experimentation*. DoD Command and Control Research Program, 2005.

3. Arlington VA Government. *Analysis of Response to Sept. 11 Pentagon Attack Shows Value of Preparedness, Challenges to Overcome*, July 2002. Published electronically at www.co.arlington.va.us/newsReleases/Scripts/ViewDetail.asp?Index=843.

4. Atkinson, Simon R. and James Maffat. *The Agile Organization*. DoD Command and Control Research Progra, 2005.

5. Beshore, David G. "Self Organizing Maps (SOMs) for Systems, Software, Management and CMMI Document Relevancy." *INCOSE 2003 - 13th Annual Internation Symposium Proceedings*. 2003.

6. Beshore, David G. "A Highly Automated CMMI-Driven Self-Organizing and Mapped (SOM) Document Library." *INCOSE 2006 - 16th Annual International Symposium Proceedings*. 2006.

7. Beshore, David G. "Top 40 Systems Engineering Work Products From Phrase Lists and Self-Organizing Maps." *INCOSE 2006 - 16th Annual International Symposium Proceedings*. 2006.

8. Bohora, Altaf S. et. al. "Integrated Peer-to-Peer Applications for Advanced Emergency Response Systems, Part I: Concept of Operations," *Proceedings of the 2003 Systems and Information Engineering Design Symposium*, 255–260 (2003).

9. Borgatti, S.P., et al., "Ucinet for Windows: Software for Social Network Analysis.." Harvard, MA: Analytic Technologies, 2002.

10. Bosch Aerospace Division. *Tethered Aerostats*. Published electronically at http://www.boschaero.com/aerostat.htm.

11. Bruno, Hal. "9/11 Commissions's parting shot Cites "Lack of Urgency" by Feds," *Firehouse*, 16 (January 2006).

12. Chairman of the Joint Chiefs of Staff, Washington DC. *Instruction 3170.01E Joint Capability and Development System*, March 2005. Published electronically at http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf.

13. Cisco Systems. *Beyond Radio: Redefining Interoperability to Enhance Public Safety*, September 2005. Published electronically at http://www.cisco.com/en/US/products/ps6718/products_white_paper0900aecd80535985.shtml.

14. Cole, Ronald A. *Survey of the State of the Art in Human Language Technology*. Published electronically at http://www.coli.uni-saarland.de/publikationen/softcopies/Cole:1997:SSA.pdf, 1997.

15. Colombi, John, "Concept Definition and System Analysis SENG 653 JCIDS Analysis Overview Lecture 2."

16. Compagnoni, Barry A. *The National Response System: The Need to Leverage Networks and Knowledge*. MS thesis, Naval Postgraduate School, March 2006.

17. Department of Defense, Washington DC. *Joint Vision 2020*. Published electronically at http://www.dtic.mil/jointvision/jvpub2.htm.

18. Department of Defense, Washington DC. *Major Combat Operations Joint Operating Concept*, September 2004. Published electronically at http://www.dtic.mil/jointvision/draftmco_joc.doc.

19. Department of Defense, Washington DC. *Capstone Concept for Joint Operations v2.0*, August 2005. Published electronically at http://www.dtic.mil/futurejointwarfare/concepts/approved_ccjov2.pdf.

20. Department of Defense, Washington DC. *Net-Centric Environment Joint Functional Concept, Version 1.0*, April 2005. Published electronically at http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf.

21. Department of Defense, Washington DC. *Net-Centric Operating Environment Joint Integrating Concept, Version 1.0*, October 2005. Published electronically at http://www.dod.mil/cio-nii/docs/netcentric_jic.pdf.

22. Department Of Defense. *Netcentric Environment Joint Functional Concept v1.0*, September 2005. Published electronically at http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf.

23. Department of Homeland Security, Washington DC. *National Strategy For Homeland Security Office Of Homeland Security*, July 2002. Published electronically at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

24. Department of Homeland Security, Washington DC. *National Incident Command System*, March 2004. Published electronically at http://www.nimsonline.com/nims_3_04/index.htm.

25. Department of Homeland Security, Washington DC. *National Incident Management System*, March 2004. Published electronically at http://www.fema.gov/pdf/emergency/nims/nims_doc_full.pdf.

26. Department of Homeland Security, Washington DC. *National Response Plan*, December 2004. Published electronically at http://www.dhs.gov/xlibrary/assets/NRPbaseplan.pdf.

27. Department Of Homeland Security, Washington DC. *Joint Field Office Activation and Operations Interagency Integrated Standard Operating Procedure* (Version 8.3 Edition), April 2006. Published electronically at http://www.dhs.gov/xlibrary/assets/NRP_JFO_SOP.pdf.

28. Department of Homeland Security. *Public Safety Statement of Requirements (SoR) for Communications and Interoperability Volume 1* (Version 1.2 Edition), October 2006. Published electronically at http://www.safecomprogram.gov/NR/rdonlyres/8930E37C-C672-48BA-8C1B-83784D855C1E/0/SoR1_v12_10182006.pdf.

29. Dunn, Vincent. "Terrorism Strategies for First-In Fire units," *Firehouse* (January 2006).

30. Eisner, Harvey. "New Orleans Firefighters Rescue Thousands by Boat," *Firehouse* (January 2006).

31. Eisner, Harvey. "You Had to See It To Believe it," *Firehouse*, 8 (January 2006).

32. Fordahl, Matthew and Bruce Meyerson. "Post Katrina: Uniform Emergency Communications Needed," *Associated Press* (September 2005).

33. GAO, "Hurricane Katrina, Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters." Published electronically at http://www.gao.gov/new.items/d06643.pdf, May 2006.

34. Garska, John and David Alberts. *Network Centric Operations Conceptual Framework, Version 2.0 (Draft)*. Technical Report, Vienna, VA: Evidence Based Research, Inc., 2004.

35. Hammer, Michael and James Champy. *Reengineering the Corporation*. Harper-Collins, 2001.

36. Hanneman, Robert A. and Mark Riddle. *Introduction to Social Network Methods*. University of California Riverside [published in digital format at http://faculty.ucr.edu/ hWong-Jirueman/], 2005.

37. Imel, Kathy J. and James W. Hart. *Understanding Wireless Communications in Public Safety A Guidebook to Technology, Issues, Planning, and Management* (Second Edition). The National Law Enforcement and Corrections Technology Center (Rocky Mountain Region).

38. JCS J-8/Force Application Assessment Division, Washington DC. *Conducting a Capabilities-Based Assessment (CBA) Under the Joint Capabilities Integration and Development System (JCIDS)*, January 2006. Published electronically at http://www.dtic.mil/futurejointwarfare/strategic/cba_guide06.pdf.

39. Jenkins, William O. Jr., "Emergency Preparedness and Response, Some Issues and Challenges Associated with Major Emergency Incidents." Published electronically at www.gao.gov/new.items/d06467t.pdf, February 2006.

40. Kennedy, Harold. “Can You Hear Me,” *National Defense*, 30–31 (July 2006).

41. Kitchenham, Barbara Ann. “Evaluating Software Engineering Methods and Tools Part 2: Selecting an appropriate evaluation method - technical criteria,” *Software Engineering Notes*, *21 no 2*:11–15 (1996).

42. Kitchenham, Barbara Ann. “Evaluating Software Engineering Methods and Tools Part3: Selecting an appropriate evaluation method - practical issues,” *Software Engineering Notes*, *21 no 4*:9–12 (1996).

43. Lancaster, David D. *Developing a Fly-Away-Kit (FLAK) to Support Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR)*. MS thesis, Naval Post Graduate School Monterey, California, June 2005.

44. The Lehigh Group. *Safe Working Loads of Rope*. Published electronically at http://www.lehighgroup.com/workingload.htm.

45. Liesenborgs, Jori, “Voice over IP in networked virtual environments,” May 2000.

46. Lucila Carvalho, Louise Scott, Ross Jeffery. “An exploratory study into the use of qualitative research methods in descriptive process modelling,” *Information and Software Technology*, *47*:113–127 (2005).

47. McGrath, Dennis, et al. “A Simple Distributed Simulation Architecture for Emergency Response Exercises.” *Proceedings of the 2005 Ninth IEEE International Symposium on Distributed Simulation and Real-Time Applications*. 2005.

48. Miller, George A. “The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information,” *Psychology Review*, *63*:81–97 (1956).

49. Moffat, James. *Complexity Theory and Net-Centric Warfare*. DoD Command and Control Research Program, 2003.

50. Motorola, Inc, “4.9 GHz Public Safety Broadband Spectrum Overview of Technical Rules And Licensing Instructions.” Published electronically athttp://www.npstc.org, January 2005.

51. Moulton, Steve, et al. “Sensor Networks for Emergency Response: Challenges and Opportunities,” *Pervasive Computing*, 16–22 (2004).

52. MSN, “Encarta.” Publised electronically at http://encarta.msn.com/dictionary_/collaborate.html, 2007.

53. Networks, Belair, “Capacity of Wireless Mesh Networks Understanding Single Radio, Dual Radio and Multi-Radio Wireless Mesh Networks.”

54. Office of the President. *Homeland Security Presidential Directive 5*, February 2003. Published electronically at http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html.

55. Office of the Secretary of Defense, Washing DC. *DoD Unmanned Systems Roadmap 2005-2030*. Published electronically at http://www.acq.osd.mil/usd/Roadmap%20Final2.pdf.

56. Ohio Department of Public Safety. *State Interoperable Communications Plan*, October 2005. Published electronically at http://ema.ohio.gov/pdfs/Ohio_Interop_appendices.pdf.

57. on Terrorist Attacks UponThe United States, National Commission. *The 9/11 Commission Report*. Published electronically at http://www.9-11commission.gov, July 2004.

58. Online, New Orleans, "New Orleans Fact and Statistics." Published Electronically at http://www.neworleansonline.com/tools/factstats.html, February 2006.

59. Perry, Walter L. and James Moffat. *Information Sharing Among Military Headquarters*. Technical Report, The RAND Corporation, 2004.

60. Program, Public Safety Wireless Network. *Answering the Call: Communications Lessons Learned from the Pentagon Attack*. Report, Public Safety Wireless Network Program, January 2002.

61. Proxim. *MeshMAX 3500WM Tri-radio, WiMAX subscriber and Wi-Fi Mesh access point*. Proxim. Published electronically at www.Proxim.com.

62. SAFECOM Program, Department of Homeland Security. *Public Safety Statement of Requirements for Communications and Interoperability, Volume 2, Version 1*, August 2006. Published electronically at http://www.safecomprogram.gov/NR/rdonlyres/B20DC842-B760-4DB0-B3B6-D3F1B0A5F26B/0/PS_SoR2_v10_9112006.pdf.

63. Systems, Cisco, "Cisco Aironet 5 GHz 54 Mbps Wireless LAN Client Adapter (CB20A)." Published electronically at http://www.cisco.com.

64. University of Hawaii, Manoa HI. *Balloon Lift With Lighter than Air Gases*. Published electronically at http://www.chem.hawaii.edu/uham/lift.html.

65. Walker, David M., "Hurricane Katrina, GAO's Preliminary Observations Regarding Preparedness, Response, and Recovery." GAO Website, March 2006.

66. Wang, Hungjen and Daniel Frey. "A Study of Applying Game Theoretic Concepts on Distributed Engineering System Design." *INCOSE 2006 - 16th Annual International Symposium Proceedings*. 2006.

67. Watts, Duncan J. *Small Worlds: The Dynamics of Networks between Order and Randomness*. Princeton University Press, 1999.

68. Werner, Charles. "Hurricane Katrina - A Time To Act," *Firehouse*, 10 – 14 (January 2006).

69. Werner, Charles. "Interoperability SWEET," *Firehouse.com* (3-30-2005).

70. West, Douglas B. *Introduction to Graph Theory*. Prentice-Hall, Inc., 2001.

71. Wikipedia, “Mean Opinion Scores,” 2007.

72. Wong-Jiru, Ann. *Graph Theoretical Analysis of Network Centric Operations Using Multi-Layer Models*. MS thesis, Air Force Institute of Technology, 2006.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* 22 Mar 07	**2. REPORT TYPE** **Master's Thesis**	**3. DATES COVERED** *(From – To)* August 06 – March 07

4. TITLE AND SUBTITLE Investigating Hastily-Formed Collaborative Networks	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Campbell, Joshua S., Captain, USAF, Cooley, Stanley L., Lt Commander, USN, Durkin, Matthew F., Maj, USAF, Maddocks, Brian K., Maj, USAF	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/ENY) 2950 Hobson Way WPAFB OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GSE/ENY/07-M01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFRL/AFOSR/IO Attn: Maj. Amy Magnus 875 N Randolph St, Suite 325, RM 3112 Arlington, VA 22203 DSN: 426-8431	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This research explores both the human and technical aspects of the network centric environment in the context of a major disaster (e.g. Hurricane Katrina) or incident of national significance. The National Incident Management System (NIMS) is viewed by the authors as a social network, and an organizational topology is developed to improve its effectiveness. A Rapid Network Deployment Kit (RNDK) using commercial-off-the-shelf (COTS) wireless networking technology is also proposed that facilitates immediate NIMS implementation. The integration of logical and technical analyses forms a comprehensive systems engineering proposal to facilitate collaboration in a net-centric environment. It is envisioned that the methodology used herein to derive and evaluate comprehensive networks proves extendable to other contexts thereby contributing to the net-centric body of knowledge.

15. SUBJECT TERMS

Hastily Formed Networks, Collaborative Networking, NIMS, National Incident Management System, Network Centric Environment, Disaster Response Network.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Lt. Col John M. Colombi
REPORT **U**	**ABSTRACT** **U**	**c. THIS PAGE** **U**	**UU**	125	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3355, ext 3347; e-mail: john.colombi@afit.edu